

## I. THE INFINITUDE OF PRIMES (The Book, chapter 1)

A **prime number** is an integer  $p > 1$  which is only divisible by  $\pm 1$  and itself. Often we just say “prime” to mean “prime number”. The set of prime numbers is denoted in The Book by

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\},$$

although this notation is not standard.

Our first theorem asserts that  $\mathbb{P}$  has infinitely many elements. We will give several different proofs of this, and each proof will tell us something new about prime numbers.

**1. Euclid’s proof and variations** — The first proof is the oldest, going back to Euclid. It is the easiest, and it proves the bare minimum. The style of the proof is by **contradiction**, in which we assume the result is false, and use that assumption to derive a contradiction.

Before giving the proof, here is the idea. Suppose we know only the primes 2,3,5,7. We can still deduce that there must be a prime beyond 7, by considering the number

$$N = 2 \cdot 3 \cdot 5 \cdot 7 + 1.$$

By adding 1, we ensure that  $N$  is not divisible by 2,3,4,5,7, so all of its prime divisors are primes  $> 7$ .

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

*Proof.* Assume there are only finitely many primes  $p_1, \dots, p_k$  and let

$$N = p_1 \cdots p_k + 1.$$

Let  $q$  be a prime divisor of  $N$ . Then  $q = p_i$  for some  $i$ , so  $q$  divides both  $N$  and  $N - 1$ , so  $q$  divides  $N - (N - 1) = 1$ , a contradiction.  $\square$

One way to understand an idea in a proof is to see what else can be proved using the same idea. Now, the primes  $p > 2$  may be partitioned into two families

$$1, 5, 13, 17, 29, \dots \quad (4k + 1 \text{ primes})$$

$$3, 7, 11, 19, 23, \dots \quad (4k + 3 \text{ primes})$$

At least one of these two families is infinite, by 1.1.

**1.2 Theorem.** *The set of primes of the form  $4k + 3$  is infinite.*

*Proof.* Assume there are only finitely many  $4k + 3$ -primes  $p_1, \dots, p_k$ . Let  $N = 4p_1 \cdots p_k - 1 = 4(p_1 \cdots p_k - 1) + 3$ . Then  $N \equiv 3 \pmod{4}$ . Now if  $a \equiv 1 \pmod{4}$  and  $b \equiv 1 \pmod{4}$  then  $ab \equiv 1 \pmod{4}$ , by (0.2). Hence there is some prime  $q$  dividing  $N$  such that  $q \equiv 3 \pmod{4}$ . Then  $q$  divides  $N$  and  $N + 1$ , so  $q \mid 1$ , a contradiction.  $\square$

In fact, there are also infinitely many  $4k + 1$ -primes, but the Euclid argument fails to prove that, since the product of  $4k + 3$  primes is not necessarily of the form  $4k + 3$ . The only other time the argument works is for  $6k + 5$  primes.

**1.3 Theorem.** *The set of primes of the form  $6k + 5$  is infinite.*

*Proof.* Same argument as 1.2, using  $N = 6p_1 \cdots p_k - 1$ .  $\square$

We cannot prove infinitude of primes in any other arithmetic progression  $ak + b$  in this way. It only works when 1 and  $a - 1$  are the only two positive integers  $< a$  and relatively prime to  $a$ , and in that case it only works for  $b = a - 1$ .

**2. Fermat numbers** — Even though there are infinitely many primes, there is no simple formula for producing prime numbers. However, Fermat observed that the numbers

$$F_n = 2^{2^n} + 1$$

are prime for  $n = 0, 1, 2, 3, 4$ . A century later, it was discovered by Euler that  $F_5 = 641 \cdot 6700417$ . So the  $F_n$ 's are not always prime. In fact no one has ever found a prime  $F_n$  for  $n > 4$ . However, the  $F_n$ 's are relatively prime among themselves. This leads to another proof of infinitude of primes, including infinitude of the  $4k + 1$  primes.

**2.1 Lemma.**  $\prod_{k=0}^{n-1} F_k = F_n - 2$ .

*Proof.* by induction.  $\square$

**2.2 Corollary.**  $(F_n, F_m) = 1$  if  $n \neq m$ .

*Proof.* We may assume  $m < n$ . By 2.1,  $F_m \mid F_n - 2$ . Hence if  $p$  divides both  $F_m$  and  $F_n$  then  $p = 2$ . But Fermat numbers are odd, so  $p \neq 2$ .  $\square$

**2.3 Corollary.** *There are infinitely many primes dividing Fermat numbers.*

*Proof.* Let  $\mathcal{F}_n = \{p \in \mathbb{P} : p \mid F_n\}$ . By Corollary 2.2, we have  $\mathcal{F}_n \cap \mathcal{F}_m = \emptyset$  if  $n \neq m$ . Hence the collection of such primes

$$\bigcup_{n=0}^{\infty} \mathcal{F}_n$$

is infinite.  $\square$

We will see later that every prime in  $\mathcal{F}_n$  is of the form  $1 + k2^{n+1}$ .

**3. Equivalence relations, groups and Lagrange's theorem** — This section is preparation for a group-theoretic proof of the infinitude of primes.

**Definition 3.1.** *A relation on a set  $S$  is a subset  $R \subset S \times S$ . We write  $a \sim b$  to mean that  $(a, b) \in R$ . The relation is an **equivalence relation** if the following three conditions hold:*

- (1) *Symmetric:*  $a \sim b \Rightarrow b \sim a$  for all  $a, b \in S$ .
- (2) *Reflexive:*  $a \sim a$  for all  $a \in S$ .
- (3) *Transitive:* If  $a, b, c \in S$  and  $a \sim b$  and  $b \sim c$ , then  $a \sim c$ .

Given an equivalence relation  $\sim$  on  $S$ , let

$$[a] = \{b \in S : a \sim b\}.$$

This is called the **equivalence class** of  $a$ .

**Theorem 3.2.**

- (1) If  $a \sim b$  then  $[a] = [b]$ , and conversely.
- (2) If  $[a] \neq [b]$  then  $[a] \cap [b] = \emptyset$ .

*Proof.* Assume  $a \sim b$ . We must show that  $[a] \subset [b]$  and  $[b] \subset [a]$ . Let  $x \in [a]$ . That means  $x \sim a$ . Since  $a \sim b$  by hypothesis, we have  $x \sim b$  by transitivity. Now let  $y \in [b]$ . That means  $y \sim b$ . Now  $b \sim a$  by reflexivity, so  $y \sim a$ , so  $y \in [a]$ . This proves  $[a] = [b]$ . Conversely, if  $[a] = [b]$ , then by definition we have  $a \sim b$ . This proves (1).

We prove (2) by contradiction. Assume  $[a] \neq [b]$ , but  $[a] \cap [b] \neq \emptyset$ . Hence there is some  $x \in [a] \cap [b]$ . Then  $x \sim a$  and  $x \sim b$ . By reflexivity and transitivity, this means  $a \sim b$ , so  $[a] = [b]$  by (1), a contradiction.  $\square$

The main point about equivalence classes is that the same class can go by different names  $[a]$  or  $[b]$ , and this happens exactly when  $a \sim b$ .

For our first example, let  $S = \mathbb{Z}$  and fix a prime  $p$ . Define  $a \sim b$  if  $a \equiv b \pmod{p}$  (in other words,  $a \sim b$  if  $p \mid (a - b)$ ). Let  $\mathbb{Z}_p$  be the set of equivalence classes. We can write the elements of  $\mathbb{Z}_p$  as

$$\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}.$$

Note that  $[p] = [0]$ ,  $[p-1] = [-1]$ , and in general,  $[a] = [b]$  if and only if  $a \equiv b \pmod{p}$ . We define addition and multiplication in  $\mathbb{Z}_p$  by

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

This makes sense, because if  $a \equiv a' \pmod{p}$  and  $b \equiv b' \pmod{p}$  then  $a + b \equiv a' + b' \pmod{p}$  and  $ab \equiv a'b' \pmod{p}$ .

For present purposes, we are interested in multiplication only. Define

$$\mathbb{Z}_p^\times = \{[1], [2], \dots, [p-1]\},$$

that is, remove  $[0]$  from  $\mathbb{Z}_p$ .

**Lemma 3.2.** *The product of two elements in  $\mathbb{Z}_p^\times$  is again in  $\mathbb{Z}_p^\times$ . For any  $[a] \in \mathbb{Z}_p^\times$  there is an element in  $\mathbb{Z}_p^\times$  whose product with  $[a]$  is  $[1]$ . This element is denoted  $[a]^{-1}$ .*

*Proof.* Let  $[a], [b] \in \mathbb{Z}_p^\times$ . If  $[a][b] \notin \mathbb{Z}_p^\times$ , we must have  $[a][b] = [0]$ , that is,  $[ab] = [0]$ . This means  $p \mid ab$ . Since  $p$  is a prime, this means either  $p \mid a$  or  $p \mid b$ , so either  $[a] = [0]$  or  $[b] = [0]$ , so either  $[a] \notin \mathbb{Z}_p^\times$  or  $[b] \notin \mathbb{Z}_p^\times$ , contradiction. This proves the first sentence in Lemma 3.2. For the second assertion, consider the powers  $[a], [a]^2, [a]^3, \dots$ . Since  $\mathbb{Z}_p^\times$  is finite, the powers must repeat, so  $[a]^i = [a]^j$  for some  $i < j$ . This means  $p \mid a^j - a^i = a^i(a^{j-i} - 1)$ . Since  $p \nmid a$ , we have  $p \mid a^{j-i} - 1$ , so  $[a]^{j-i} = [1]$ , so  $[a][a]^{j-i-1} = [1]$ . Thus,  $[a]^{-1} = [a]^{j-i-1}$ .  $\square$

**Definition 3.3.** *A group is a set  $G$  together with a way of combining two elements  $g, h \in G$  into a third element  $gh$  in  $G$  such that the following three properties hold.*

- (1) *Associativity:*  $(gh)k = g(hk)$  for all  $g, h, k \in G$ .
- (2) *Identity Element:* There is an element  $e \in G$  such that  $ge = eg = g$  for all  $g \in G$ .
- (3) *Inverses:* For every  $g \in G$  there is an element in  $G$  whose product with  $g$  (on either side) is  $e$ . This element is denoted  $g^{-1}$ .

The **order** of  $G$  is the number of elements in  $G$ , denoted by  $|G|$ .

We have proved in 3.2 that  $\mathbb{Z}_p^\times$  is a group (associativity is left as an exercise). We have

$$|\mathbb{Z}_p^\times| = p - 1.$$

In  $\mathbb{Z}_p^\times$ , the order of multiplication does not matter. That is,  $[a][b] = [b][a]$ . A group with this property is called an **abelian group**.

An example of a non-abelian group is given by the set  $S_3$  of permutations of  $\{1, 2, 3\}$ , where the multiplication is composition. Thus,  $gh$  is the permutation  $g \circ h$ , i.e.,  $h$  followed by  $g$ . This group is called the **symmetric group** on three objects. Note that the permutation that switches 1 and 2 does not commute with the permutation that switches 2 and 3. So  $S_3$  is non-abelian.

Another example of a group is the set  $GL_2$  of all  $2 \times 2$  invertible matrices, where the “multiplication” is matrix multiplication. The identity element is the identity matrix. Since matrix multiplication is non-commutative, the group  $GL_2$  is also non-abelian.

**Definition 3.4.** A **subgroup** of a group  $G$  is a subset  $H \subset G$  with the following properties

- (1) *Closure* If  $h, h' \in H$  then  $hh' \in H$
- (2) *Identity* The identity element  $e$  of  $G$  is contained in  $H$ .
- (3) *Inverses* If  $h \in H$  then  $h^{-1}$  is also in  $H$ .

For example, if  $g \in G$ , the set  $\langle g \rangle$  of all powers of  $g$  is in  $G$ . If  $G$  is finite, then  $g^{-1}$  can be expressed as a positive power of  $g$  (imitate the proof of 3.2) so we have

$$\langle g \rangle = \{g, g^2, \dots, g^m = e\}$$

where  $m$  is the smallest power of  $g$  such that  $g^m = e$ . This number  $m$  is called the **order** of the element  $g$ . Note that  $m$  is also the order of the subgroup  $\langle g \rangle$ , as defined after Definition 3.3.

For example  $\mathbb{Z}_7^\times$  is a group of order 6. It has one subgroup of order 2, namely  $\langle [2] \rangle$  and one subgroup of order 3, namely  $\langle [3] \rangle$ . The group  $S_3$  also has order 6, but it has three subgroups of order two (generated by the three possible switches) and one subgroup of order 3, generated by the cycle.

The main theorem that ties together the ideas of equivalence relation and group is the following.

**Lagrange’s Theorem 3.4.** If  $G$  is a finite group and  $H$  is a subgroup of  $G$  then  $|H|$  divides  $|G|$ . In particular, the order of any element of  $G$  divides  $|G|$ .

*Proof.* Define a relation on  $G$  by  $g \sim g'$  if  $g' = gh$  for some  $h$  in  $H$ . The group properties ensure that  $\sim$  is an equivalence relation. The equivalence classes are the sets  $gH = \{gh : h \in H\}$  each of which has  $|H|$  elements. If  $n$  is the number of equivalence classes, then  $|G| = n|H|$ , so  $|H|$  divides  $|G|$ .  $\square$

**Corollary 3.5.** For every  $g \in G$ , we have  $g^{|G|} = e$ .

*Proof.* Let  $m$  be the order of  $g$  and let  $n = |G|/m$ . Consider the subgroup  $H = \langle g \rangle$ . We have  $g^{|G|} = g^{mn} = (g^m)^n = e^n = e$ .  $\square$

Here is useful related fact, having nothing to do with Lagrange.

**Lemma 3.6.** *If  $g^k = e$ , then  $m \mid k$ , where  $m$  is the order of  $g$ .*

*Proof.* Note that  $m \leq k$ , by the definition of order. Suppose  $m \nmid k$ , and divide  $m$  into  $k$  and take the remainder:

$$k = qm + r, \quad 0 < r < m.$$

Then

$$e = g^k = g^{qm+r} = (g^m)^q g^r = g^r,$$

since  $g^m = e$ . But this contradicts the minimality of  $m$ .  $\square$

If we apply 3.5 to the group  $G = \mathbb{Z}_p^\times$  and an element  $[a] \in \mathbb{Z}_p^\times$ , we get the following corollary.

**Fermat's Little Theorem 3.6.** *If  $p \nmid a$  then  $a^{p-1} \equiv 1 \pmod{p}$ .*

**4. Mersenne Numbers** — For any prime  $p$ , the number

$$M_p = 2^p - 1$$

has a good chance of being prime as well. This gives a possible way to produce big primes from small primes. It does not always work. For the first ten primes  $p = 2, 3, \dots, 29$ , we have

$$\begin{aligned} M_2 &= 3 && \text{prime} \\ M_3 &= 7 && \text{prime} \\ M_5 &= 31 && \text{prime} \\ M_7 &= 127 && \text{prime} \\ M_{11} &= 2047 = 23 \cdot 89 \\ M_{13} &= 8191 && \text{prime} \\ M_{17} &= 131071 && \text{prime} \\ M_{19} &= 524287 && \text{prime} \\ M_{23} &= 8388607 = 47 \cdot 178481 \\ M_{29} &= 536870911 = 233 \cdot 1103 \cdot 2089. \end{aligned}$$

Lagrange tells us something about the possible prime divisors of  $M_p$ .

**Theorem 4.1.** *If  $p > 2$  and  $q$  are primes, and  $q \mid M_p$  then  $q = 1 + 2kp$  for some integer  $k$ .*

*Proof.* If  $q \mid 2^p - 1$ , then  $[2]^p = [1]$  in  $\mathbb{Z}_q^\times$ , so by 3.?, the order of  $[2]$  in  $\mathbb{Z}_q^\times$  divides  $p$ . Since  $p$  is a prime, and  $[2] \neq [1]$ , the order must be  $p$ . By 3.? we have then  $p \mid q - 1$ , so  $q = 1 + np$  for some integer  $n$ . If  $n$  were odd then  $q$  would be even, hence  $q = 2$ , impossible since  $q \mid M_p$  and  $M_p$  is odd. Hence  $n = 2k$  for some integer  $k$ .  $\square$

This gives a method for factoring, or proving primality of  $M_p$ . Given  $p$ , compute  $1 + 2p, 1 + 4p, \dots$  to the last number of this form which is less than  $2^{p/2}$ . Discard the non-prime numbers on the list. The remaining numbers include all the possible prime divisors of  $M_p$ ; you can then check these directly.

**Corollary 4.2.** *Given any prime  $p$ , there is another prime  $q$  of the form  $1 + 2kp$ . In particular, we see again that there must be infinitely many primes.*

**5. Fermat Numbers again** — We can also use Lagrange to say something about the prime divisors of Fermat numbers  $F_n = 2^{2^n} + 1$ .

**Theorem 5.1.** *If the prime  $p$  divides  $F_n$ , then  $p = 1 + k2^{n+1}$  for some integer  $k$ .*

*Proof.* If  $p \mid 2^{2^n} + 1$  then  $p \mid 2^{2^{2n}} - 1$ . Let  $m$  be the order of  $[2]$  in  $\mathbb{Z}_p^\times$ . Then  $m \mid 2^{2n}$ , so  $m = 2^\ell$  for some integer  $\ell \leq 2n$ . Then  $p \mid 2^{2^\ell} - 1 = (2^{2^{\ell-1}} + 1)(2^{2^{\ell-1}} - 1)$ . Here  $p$  cannot divide the second factor because  $2^\ell$  is the order of  $2 \pmod p$ . Hence  $p$  divides the first factor, which is  $F_{\ell-1}$ . But  $p$  also divides  $F_n$ , so  $\ell - 1 = n$  by (2.?). Hence  $\ell = n + 1$ , so  $m = 2^\ell = 2^{n+1}$ . By Lagrange,  $m \mid p - 1$ , so  $p - 1 = km = k2^{n+1}$  for some integer  $k$ .  $\square$

Recall that  $\mathcal{F}_n$  denotes the set of prime divisors of  $F_n$ .

**Corollary 5.2.** *For any  $d > 1$ , the set*

$$\bigcup_{n \geq d-1} \mathcal{F}_n$$

*consists of infinitely many primes of the form  $1 + k2^d$ .*

This shows, for example that there are infinitely many primes of the form  $1 + 4k$ , in fact infinitely many primes of the form  $1 + 8k$ , in fact infinitely many primes of the form  $1 + 16k$ , etc.

**6. Review of infinite series** — This section is preliminary to an analytic approach to the infinitude of primes.

An infinite series  $\sum_{k \geq 0} a_k$  is said to **converge** if the sequence of partial sums

$$a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots \tag{6a}$$

converges to a number  $L$ , in which case we call this  $L$  the **sum** of the series, and write

$$\sum_{k=0}^{\infty} a_k = L.$$

If  $a_k \geq 0$  for all  $n$ , the number  $L$  can be understood in terms of length, as follows. The series converges exactly when there is a number  $M$  which is  $\geq$  each partial sum in (6a). Any such  $M$  is called an **upper bound** on the partial sums. The number  $L$  is then the smallest such upper bound (“least upper bound”). That is,  $L$  is the smallest number which is larger than every partial sum in (6a). If there is no number larger than every partial sum, the series diverges, and there is no sum. We will indicate this, in the case where all  $a_k \geq 0$ , by writing

$$\sum_{k=0}^{\infty} a_k = \infty.$$

Three kinds of series are most important for us.

i) Geometric series

$$\sum_{k=0}^{\infty} x^k = \begin{cases} \frac{1}{1-x} & \text{if } |x| < 1 \\ \text{diverges} & \text{if } |x| \geq 1. \end{cases}$$

*Proof.* : The partial sums

$$1 + x + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x} \rightarrow \frac{1}{1 - x}, \quad \text{if } |x| < 1,$$

and diverges otherwise.  $\square$

ii) Harmonic series

$$\sum_{k=1}^{\infty} \frac{1}{k} = \infty.$$

*Proof.* For each  $x \in [k, k + 1]$ , we have  $\frac{1}{k} \geq \frac{1}{x}$ . Hence

$$\sum_{k=1}^n \frac{1}{k} \geq \int_1^{n+1} \frac{1}{x} dx = \log(n + 1) \rightarrow \infty.$$

$\square$

iii) Zeta series (or Zeta function)

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} \quad \text{converges for } s > 1.$$

*Proof.* Assume  $s > 1$ . For  $k \geq 2$  and  $x \in [k - 1, k]$ , we have  $\frac{1}{k} \leq \frac{1}{x}$ , so

$$\sum_{k=1}^n \frac{1}{k^s} = 1 + \sum_{k=2}^n \frac{1}{k^s} \leq 1 + \int_1^n \frac{1}{x^s} dx \leq 1 + \int_1^{\infty} \frac{1}{x^s} dx = \frac{s}{s - 1}.$$

Thus  $\frac{s}{s-1}$  is an upper bound for all the partial sums in the zeta series. Hence the zeta series converges to some number  $\zeta(s)$ , which is less than  $\frac{s}{s-1}$ .  $\square$

Note that as  $s \rightarrow 1$ , the upper bound  $\frac{s}{s-1}$  goes off to infinity, in accordance with the divergence of the harmonic series. We only know the actual values of  $\zeta(s)$  for certain values of  $s$ . This is an upcoming topic.

**7. Big and small sets of positive integers** — Suppose  $S \subset \mathbb{N}$ , and consider the sum

$$\sum_{k \in S} \frac{1}{k}. \tag{7a}$$

If the sum (7a) diverges, we say  $S$  is “big”. If (7a) converges, we say  $S$  is “small”. Clearly a finite set  $S$  is small. The big/small dichotomy is only interesting for infinite sets.

For example  $\mathbb{N}$  itself is big, because the harmonic series diverges. The set

$$S = \{2, 4, 6, 8, \dots\}$$

is also big, because

$$\sum_{k=1}^n \frac{1}{2k} = \frac{1}{2} \sum_{k=1}^n \frac{1}{k} \rightarrow \infty.$$

Likewise,  $S = \{1, 3, 5, 7, 9, \dots\}$  is big because

$$\sum_{k=1}^n \frac{1}{2k+1} > \sum_{k=1}^n \frac{1}{2k+2} = \frac{1}{2} \sum_{k=2}^n \frac{1}{k} \rightarrow \infty.$$

On the other hand, the sets

$$S_1 = \{1, 2, 4, 8, 16, \dots\}$$

$$S_2 = \{1, 3, 9, 27, \dots\}$$

$$S_3 = \{1, 4, 9, 16, \dots\}$$

are all small, since the corresponding sums (7a) are geometric with  $x = \frac{1}{2}$ , geometric with  $x = \frac{1}{3}$  and zeta(2), respectively.

For a less obvious example, let  $S$  be the set of  $k \in \mathbb{N}$  which have no zero in their decimal expansion. This seems like almost all of the integers. Let  $S_n$  be the set of  $k \in S$  having exactly  $n$  digits.

$$\sum_{k \in S} \frac{1}{k} = \sum_{n=1}^{\infty} \sum_{k \in S_n} \frac{1}{k}.$$

We cannot compute this sum exactly, but if we ask for less, namely an estimate, then we are rewarded by a geometric series, which we can compute. This is a common theme in analysis. Consider some  $k \in S_n$ . Since each digit of  $k$  is nonzero, we have

$$k \geq 111 \cdots 1 = 1 + 10 + 10^2 + \cdots + 10^{n-1} = \frac{10^n - 1}{10 - 1},$$

so

$$\frac{1}{k} \leq \frac{9}{10^n - 1}$$

Since there are  $9^n$  numbers in  $S_n$ , we have

$$\sum_{k \in S_n} \frac{1}{k} < 9^n \cdot \frac{9}{10^n - 1} \leq \frac{9^n}{10^{n-1}},$$

(since  $10^n - 1 \geq 9 \cdot 10^{n-1}$ ) so

$$\sum_{k \in S} \frac{1}{k} < 9 \sum_{n=1}^{\infty} \left(\frac{9}{10}\right)^{n-1} = 90.$$

Hence  $S$  is small. This means that the set of positive integers that *do* have a zero in their decimal expansion must be big.

**8. Euler's view of the infinitude of primes** — Let  $\mathbb{P}$  be the set of prime numbers. Is  $\mathbb{P}$  big or small? First, let's look at numerical evidence. Let  $p_1, p_2, \dots$  be the primes listed in increasing order. Let

$$S(n) = \sum_{i=1}^n \frac{1}{p_i} = \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p_n}.$$

We use a computer to find

$$\begin{aligned} S(10) &= 1.5334\dots \\ S(100) &= 2.1063\dots \\ S(1000) &= 2.4574\dots \\ S(10000) &= 2.7092\dots \\ S(100000) &= 2.9061\dots \end{aligned}$$

The last one took about 70 minutes on a Mac G3. Incidentally,  $p_{100000} = 1299709$ . Even though Euler did not have access to such calculations, the question of convergence was answered by Euler. It turns out that, in fact, the sum diverges. The Book proof here was published by Erdos in 1938. It is short and elementary, with the pricetag of being extremely clever.

**Theorem 8.1.** *The set of all prime numbers is big. In other words,*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty.$$

*Proof.* Assume  $\sum_{p \in \mathbb{P}} \frac{1}{p}$  converges. Number the primes  $p_1, p_2, \dots$  in increasing order. Then there is a number  $k$  such that the tail of the series is small, say less than  $\frac{1}{2}$ :

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Call  $p_1, \dots, p_k$  the *small primes* and  $p_{k+1}, p_{k+2}, \dots$  the *big primes*.

We consider an as-yet-unspecified positive integer  $N$ . Later we will make a specific choice of  $N$ , but this choice will be shown to us by the proof, so we won't make the choice just now. Note that the choice of  $k$  was made first, using the convergence assumption, so  $k$  does not depend on  $N$ .

Now

$$N = |\{n \in \mathbb{N} : n \leq N\}|.$$

We break the set  $T = \{n \in \mathbb{N} : n \leq N\}$  into two parts,  $T = T_s \cup T_b$ , where  $T_s$  consists of the numbers in  $T$  which are divisible only by small primes, and  $T_b$  consists of the numbers in  $T$  which are divisible by at least one big prime. Then

$$N = N_b + N_s,$$

where  $N_b = |T_b|$ ,  $N_s = |T_s|$ .

We now estimate  $N_b$ . Every number in  $T_b$  is a multiple of some big prime  $p_i$ . That is,

$$T_b = \{n \leq N : p_{k+1} \mid n\} \cup \{n \leq N : p_{k+2} \mid n\} \cup \dots$$

The multiples of  $p_i$  which are  $\leq N$  are  $p_i, 2p_i, \dots, m_i p_i$  where  $m_i p_i$  is the largest multiple of  $p_i$  which is  $\leq N$ . That means  $m_i$  is the largest integer  $\leq \frac{N}{p_i}$ . The notation for the largest integer  $\leq x$ , for any number  $x$ , is  $\lfloor x \rfloor$ . So there are  $m_i = \lfloor \frac{N}{p_i} \rfloor$  multiples of  $p_i$  which are  $\leq N$ . Therefore

$$N_b \leq \sum_{i=k+1}^{\infty} \lfloor \frac{N}{p_i} \rfloor \leq \sum_{i=k+1}^{\infty} \frac{N}{p_i} = N \sum_{i=k+1}^{\infty} \frac{1}{p_i} \leq \frac{N}{2}.$$

We will next estimate  $N_s$ . First, any  $n \in \mathbb{N}$  can be expressed uniquely in the form  $n = ab^2$  where  $a$  has no square factors. In fact  $a$  is the product of those primes appearing in  $n$  with odd exponent. To estimate  $N_s$ , we count the possibilities for  $a$  and  $b$  when  $n \in T_s$ . Each  $a$  is the product of some subset of  $\{p_1, \dots, p_k\}$ , so there are  $2^k$  possibilities for  $a$ . Each  $b$  satisfies  $b^2 = \frac{n}{a} \leq \frac{N}{a} \leq N$ , so  $b \leq \sqrt{N}$ . Hence there are  $2^k \sqrt{N}$  choices for  $n \in T_s$ . In other words,

$$N_s \leq 2^k \sqrt{N}.$$

Putting our estimates together, we have

$$N = N_b + N_s \leq \frac{N}{2} + 2^k \sqrt{N}.$$

Solving for  $N$ , we get

$$\sqrt{N} \leq 2^k. \tag{8a}$$

Since  $N$  has not been specified, it follows that (8a) is true for any  $N$ . But we can make  $\sqrt{N}$  as big as we please, so if we choose  $N$  large enough, then (8a) will be violated. That is a contradiction. Therefore, the sum  $\sum_{p \in \mathbb{P}} \frac{1}{p}$  diverges.  $\square$

In essence, the assumption of convergence gave us  $k$ , which led to the impossible bound (8a) on  $N$ .

**9. The growth of primes** — Another way to measure the primes is to study the function

$$\pi(N) = \{p \in \mathbb{P} : p \leq N\}.$$

As far as I know, there is no formula for  $\pi(N)$  that is more efficient than simply counting the primes  $p \leq N$ . But we can get an estimate, using Erdos' counting method in Theorem 8.1.

Take  $N \in \mathbb{N}$ , and let  $p_1, \dots, p_k$  be the primes  $\leq N$ . So  $k = \pi(N)$ , and these are the only possible prime divisors of  $N$ . As in 8.1, for each  $n \leq N$ , we have  $n = ab^2$  uniquely, where  $a$  has no square factors. There are  $2^k$  choices for  $a$ , and  $b^2 = n/a \leq N$ , so  $b \leq \sqrt{N}$ , hence  $N \leq 2^k \sqrt{N}$ . Solving for  $k = \pi(N)$ , we get

$$\pi(N) \geq \frac{\log(N)}{\log 4}. \tag{9a}$$

So  $\pi(N)$  grows at least as fast as a constant times  $\log(N)$ . A similar estimate for  $\pi(N)$  is proved in the Book, using Calculus.

A more precise result on the growth of  $\pi(N)$  is the **Prime Number Theorem**, which was conjectured by Gauss, based on massive puffy-sleeve calculations, and finally proved in 1896 by Hadamard (France) and de la Vallée-Poussin (Belgium) independently. (How annoying that must have been!)

**Prime Number Theorem 9.1.** *We have*

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\log n} = 1.$$

Roughly speaking, this says that the function  $\pi(n)$  looks more and more like  $\frac{n}{\log n}$ , for larger and larger  $n$ . Hence, viewed up close, the graph of  $\pi(n)$  looks very jagged and random. But viewed from very far away,  $\pi(n)$  looks like  $\frac{n}{\log n}$ , which itself looks almost like a straight line, since  $n$  dominates  $\log n$ .

This theorem is too hard for us to prove in this course. Here is a table of numerical evidence for it.

$n$	$\pi(n)$	$\frac{n}{\log n}$	$\frac{\pi(n)}{n/\log n}$
10	4	4.34294	0.921
100	25	21.7147	1.151
1000	168	144.765	1.160
10000	1229	1085.74	1.131
100000	9592	8685.89	1.104
1000000	78498	72382.4	1.084
10000000	664579	620421.0	1.071
100000000	5761455	5428681.02	1.061
1000000000	50847534	48254942.4	1.053
10000000000	455052511	434294481.9	1.047

This table is misleading in one respect. It gives the impression that  $\pi(n) > \frac{n}{\log n}$  for large  $n$ , and that  $\pi(n)$  steadily decreases down toward  $\frac{n}{\log n}$ . But if you go much farther out, there is some enormous  $n$  for which  $\pi(n) < \frac{n}{\log n}$ . No one has found this  $n$ , but it was proved to exist by Littlewood (England, 1930). I think this is a beautiful demonstration of how any table of numerical evidence, no matter how large, can only consist of small cases, as far as the infinitude of integers is concerned, and therefore cannot be trusted.

**10. Some famous unsolved problems** — These problems stem, in part, from the desire for, or fear of, an efficient prime-producing machine.

**Problem 10.1.** *Are there infinitely many Fermat primes?*

So far,  $F_0, F_1, F_2, F_3, F_4$  are the only Fermat numbers which are known to be prime. Factoring larger Fermat numbers is a small industry these days, as a test of networked computation.

**Problem 10.2.** *Are there infinitely many Mersenne primes?*

In contrast to Fermat primes, Mersenne primes appear to be abundant. Every year or two someone, or some networked group of PCs, finds another largest known prime, and it is always a Mersenne prime.

**Problem 10.3.** *Which polynomials take on infinitely many prime values?*

We have seen that the polynomials  $x, 4x + 1, 4x + 3, 6x + 5, 8x + 1, 16x + 1$  etc. take on infinitely many prime values. Our best theorem in this direction is

**Dirichlet's Theorem on Arithmetic Progressions, 1837.** *If  $a$  and  $b$  are relatively prime, then the polynomial  $ax + b$  takes on infinitely many prime values.*

In other words, any linear polynomial that has a chance to produce primes will produce infinitely many primes. The next case is quadratic polynomials, but no one even knows if  $x^2 + 1$  produces infinitely many primes.

**Problem 10.4.** *Are there infinitely many twin primes? (A twin prime is a pair of consecutive odd prime numbers, like  $(41, 43)$ .)*

In contrast to the set of all primes, the set of twin primes is known to be small (Viggo Brun, 20th century), that is, the sum of  $\frac{1}{p}$  over the twin primes converges. However, this does not answer problem 4. In fact, there is a lot of experimental evidence in favor of the infinitude of twin primes, but we have seen that this can be misleading.

**Problem 10.5.** *What is the best possible error estimate in the prime number theorem?*

That is, how well can we predict the right hand column in the table in section 9? This problem boils down to the *Riemann hypothesis*, perhaps the most famous unsolved problem in all of mathematics, and a topic of vigorous research these days (without any real progress, as far as I know). Though we will not discuss the Riemann hypothesis in this course, it has to do with the zeta function  $\zeta(s)$ , which is the next topic.