Chapter 6
Primes of the form $4k + 1$

The main goal of this chapter is to prove that there are infinitely many primes of the form $4k + 1$. We model the proof of this fact on Euclid's proof of the infinitude of prime numbers which we explain. We then discuss quadratic residues and study their basic properties. We state, and prove in the next chapter, the Law of Quadratic Reciprocity. At the end of the chapter we use the Law of Quadratic Reciprocity to prove the infinitude of primes of the form $3k + 1$. In the Notes, we discuss Euclid's original writing of his proof of the infinitude of prime numbers, talk about primality testing, and review some recent progress on the Twin Prime Conjecture.

6.1 Euclid's theorem on the infinitude of primes

We saw in Chapter 5 that in order for a prime to divide the side length of a primitive right triangle, it has to be of the form $4k + 1$. It would be extremely surprising, and rather unfortunate, if there were only finitely many such primes. In this chapter we will prove the following theorem:

Theorem 6.1. *There are infinitely many primes of the form* $4k + 1$.

In general it is actually quite hard to prove there are infinitely many primes of a special form. For example, at the time of this writing it is not known if there are infinitely many primes of the form $n^2 + 1$ (Landau's Conjecture, Notes to Ch. 5), or that there are infinitely many primes p such that $p + 2$ is also prime (Twin Prime Conjecture, Notes to this chapter), or that there are infinitely many primes p such that $2p + 1$ is prime (Infinitude of Sophie Germain Primes), etc. Even the proof of the existence of infinitely many primes without any additional restrictions is a non-trivial result that requires a real idea. This goes back to Euclid, and the proof we present here is essentially Euclid's original argument [20, Book IX, Proposition 20].

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_6

Theorem 6.2 (Euclid). *There are infinitely many prime numbers.*

Proof. Suppose not, and let $\{p_1, \ldots, p_m\}$ be the (finite) set of all prime numbers. Let

$$M = p_1 \cdots p_m + 1.$$

The number M is not divisible by any of the primes p_i, but M is divisible by some prime q, which is necessarily one p_i's. In particular, $q \mid p_1 \cdots p_m$. Consequently,

$$q \mid M - p_1 \cdots p_m = 1.$$

But 1 is not divisible by any primes. This is a contradiction. □

One can try to adapt this argument to prove Theorem 6.1. So let's suppose that $\{p_1, \ldots, p_m\}$ is the finite set of primes of the form $4k + 1$, and set

$$M = p_1 \cdots p_m + 1.$$

We would then ask if this number, for some reason, has to have a new prime factor of the form $4k + 1$. It is wise to do some experiments. Let us start with the first two primes of the form $4k + 1$, namely 5 and 13. Then,

$$M = 5 \times 13 + 1 = 66 = 2 \times 3 \times 11,$$

none of whose factors are of the desired type, as $3 = 0 \times 4 + 3$ and $11 = 2 \times 4 + 3$. One might complain that the issue with this approach was that the resulting number M is not of the form $4k + 1$—in fact, it is always even. So it makes sense to define M this way:

$$M = 4p_1 \cdots p_m + 1.$$

This idea fails too. For example, the numbers 5 and 17 are both primes of the form $4k + 1$. We have

$$M = 4 \times 5 \times 17 + 1 = 341 = 11 \times 31.$$

The primes 11 and 31 are both of the form $4k - 1$. The problem is that when we multiply two primes of the form $4k - 1$, or of the form $4k + 3$, we get a number of the form $4k + 1$:

$$(4m - 1)(4n - 1) = 16mn - 4m - 4n + 1 = 4(4mn - m - n) + 1.$$

But not all is lost! In fact, this last computation suggests that maybe instead of proving the infinitude of primes of the form $4k + 1$, Euclid's idea can be adapted to prove the infinitude of primes of the form $4k - 1$. The key observation is that when we multiply numbers of the form $4k + 1$ the result is always a number of the form $4k + 1$, i.e.,

$$(4m + 1)(4n + 1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1. \qquad (6.1)$$

Theorem 6.3. *There are infinitely many primes of the form* $4k-1$.

Proof. Let $p_1, \ldots, p_m$ be a finite set of primes of the form $4k-1$. Let

$$M = 4p_1 \cdots p_m - 1.$$

The number M is of the form $4k-1$, and not divisible by any of the primes $p_1, \ldots, p_m$. Also, not all of M's prime factors can be of the form $4k+1$, because in that case by Equation (6.1) M would be of the form $4k+1$. As a result M has a prime factor of the form $4k-1$ and we have found a new prime of the desired form. □

Going back to Theorem 6.1, the idea is to find an expression M in terms of $p_1, \ldots, p_m$, which is odd, not divisible by any of the p_i's, and provably possessing a new prime factor of the form $4k+1$. One way to do this to make sure that M has *no* prime factors of the form $4k-1$. The key to making this happen is Lemma 5.6 of Chapter 5.

Proof of Theorem 6.1. Let $p_1, \ldots, p_m$ be the set of all primes of the form $4k+1$. Let

$$M = (2p_1 \cdots p_m)^2 + 1.$$

This number is not divisible by any of the p_i. It is odd, and by Lemma 5.6 none of its prime factors can be of the form $4k-1$. Every prime factor of M is new prime number of the form $4k+1$. □

For example, the numbers $5, 13, 17, 29, 37$ are all primes of the form $4k+1$. Then

$$(2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37)^2 + 1 = 233 \cdot 593 \cdot 3301 \cdot 12329,$$

with the factors on the right all being prime numbers of the form $4k+1$.

6.2 Quadratic residues

The main point of the proof of Theorem 6.1 is that a number of the form n^2+1 cannot have any prime factors of the form $4k-1$. This suggests that one may be able to prove the infinitude of other sets of prime numbers by exploring prime factors of numbers of the form $n^2 - a$ for integers a. In the argument above, $a = -1$.

Question 6.4. For an integer a, for what primes p, are there no integers n such that $p \mid n^2 - a$?

Gauss systematically studied this question, [21, §IV, Article 95], and proved a number of fundamental results. Let p be an odd prime. Suppose p does not divide a, and define the *Legendre symbol*, or the *quadratic residue symbol*, by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \exists n, n^2 \equiv a \bmod p; \\ -1 & \text{otherwise.} \end{cases}$$

If $p \mid a$, we set

$$\left(\frac{a}{p}\right) = 0.$$

We call an integer a a *quadratic residue modulo* p if $p \nmid a$ and the equation $x^2 \equiv a \bmod p$ is solvable, i.e., if $\left(\frac{a}{p}\right) = +1$. It is clear that if $a \equiv b \bmod p$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

so we often think of $\left(\frac{\cdot}{p}\right)$ as a function on the set of congruence classes modulo p.

Sometimes, when there is no danger of confusion, we write (a/p) instead of $\left(\frac{a}{p}\right)$.

Lemma 6.5 (Euler). *Let p be an odd prime. We have*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Proof. If $a \equiv 0 \bmod p$, the lemma is obvious. So we assume $a \not\equiv 0 \bmod p$. Let g be a primitive root modulo p. Then if $a \equiv g^i \bmod p$, we have

$$\left(\frac{a}{p}\right) = (-1)^i.$$

If i is even,

$$a^{\frac{p-1}{2}} \equiv g^{i\frac{p-1}{2}} \equiv g^{\frac{i}{2}\cdot(p-1)} \equiv 1 \mod p.$$

On the other hand, if i is odd,

$$a^{\frac{p-1}{2}} \equiv g^{i\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \mod p.$$

As we saw in the proof of Lemma 5.6

$$g^{\frac{p-1}{2}} \equiv -1 \mod p,$$

and this finishes the proof. □

Lemma 6.6. *Let p be an odd prime. For all integers a, b,*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \tag{6.2}$$

Proof. By Lemma 6.5 we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

This means

$$p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Since the possible values of the quadratic residue symbol are $+1, -1$, the expression on the right can take values $+2, 0, -2$. Of these numbers, the only one that is divisible by p is 0, and this observation proves the identity. □

The following lemma is a reformulation of Corollary 5.8.

Lemma 6.7. *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{6.3}$$

Proof. By Lemma 6.5 we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p.$$

Now an argument similar to the proof of Lemma 6.6 gives the lemma. □

This last statement means that there is an n such that $n^2 \equiv -1 \bmod p$ precisely when

$$(-1)^{\frac{p-1}{2}} = +1,$$

i.e., when $(p-1)/2$ is even, which is equivalent to p being of the form $4k+1$. For example, 13 and 17 are primes of the form $4k+1$ and $5^2 \equiv -1 \bmod 13$ and $4^2 \equiv -1 \bmod 17$.

These facts are enough to compute quadratic residues modulo every prime number. Let us illustrate this by computing $\left(\frac{15}{31}\right)$. By Equation (6.2) we have

$$\left(\frac{15}{31}\right) = \left(\frac{3}{31}\right)\left(\frac{5}{31}\right).$$

To compute $\left(\frac{3}{31}\right)$, we write

$$\left(\frac{3}{31}\right) \equiv 3^{\frac{31-1}{2}} \equiv 3^{15} \equiv 27^5 \equiv (-4)^5 \equiv -4^5$$

$$\equiv -4^3 \cdot 4^2 \equiv -2 \cdot 16 \equiv -1 \mod 31.$$

This means, $\left(\frac{3}{31}\right) = -1$. Next,

$$\left(\frac{5}{31}\right) \equiv 5^{\frac{31-1}{2}} \equiv 5^{15} \equiv (5^3)^5 \equiv 125^5 \equiv 1^5 \equiv 1 \mod 31.$$

Consequently, $\left(\frac{5}{31}\right) = +1$. Putting everything together,

$$\left(\frac{15}{31}\right) = \left(\frac{3}{31}\right)\left(\frac{5}{31}\right) = (-1)\cdot(+1) = -1.$$

To see a slightly more complicated example, we also compute $\left(\frac{17}{31}\right)$. By Lemma 6.5 we have

$$\left(\frac{17}{31}\right) \equiv 17^{\frac{31-1}{2}} \equiv 17^{15} \equiv (17^5)^3 \equiv 26^3 \equiv (-5)^3 \equiv -1 \mod 31.$$

As a result,

$$\left(\frac{17}{31}\right) = -1.$$

Equation (6.2) shows that in order to compute quadratic residues modulo p, we need to know $\left(\frac{q}{p}\right)$ for primes p. At first glance, $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ should have no relationship with each other—we often think of primes numbers as *independent* of each other, and in many situations they behave as if they are completely unaware of each other's presence. However, in this case, primes p and q, knowing either of $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$, tells us the value of the other one. The exact relationship was conjectured by Euler around 1745, and was proved rigorously for the first time by Gauss in 1796, though Legendre had proved some special cases as early as 1785. By the time he died, Gauss had produced eight different proofs for the theorem, the *Law of Quadratic Reciprocity*.

Theorem 6.8 (Law of Quadratic Reciprocity).

1. *If p, q are distinct odd primes, then*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right);$$

   Explicitly, $(p/q) = -(q/p)$ only when $p \equiv q \equiv 3 \bmod 4$, and in all other situations $(p/q) = (q/p)$.
2. *If p is an odd prime,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

   Explicitly written out, this means if $p \equiv 1, 7 \bmod 8$, then 2 is a quadratic residue modulo p, and if $p \equiv 3, 5 \bmod 8$, it is not.

Even though at the time of this writing there are literally hundreds of proofs of this fundamental fact available in print, unfortunately, none of them are trivial. In the next chapter we will present one of Gauss's original proofs using quadratic Gauss sums. The Law of Quadratic Reciprocity is a truly impressive theorem. This theorem has now been generalized magnificently through the works of Artin, Hilbert, and Langlands [75], and has inspired an incredible amount of mathematics. In fact, the works of four Fields medalists (V. Drinfeld, L. Lafforgue, B. C. Ngô, and M. Bhargava) have been directly or indirectly inspired by Gauss's work on the Law of Quadratic Reciprocity and its generalizations. This is indeed one of the most important theorems in all of mathematics.

One consequence of Theorem 6.8 is that it allows one to compute (a/p) very quickly. For example, suppose we want to compute (194/7919). By Equation (6.2) we have

$$\left(\frac{194}{7919}\right) = \left(\frac{2}{7919}\right)\left(\frac{97}{7919}\right).$$

By the second part of the theorem,

$$\left(\frac{2}{7919}\right) = (-1)^{(7919^2-1)/8} = (-1)^{7838820} = +1.$$

Next, by the first part,

$$\left(\frac{97}{7919}\right) = (-1)^{(97-1)(7919-1)/4}\left(\frac{7919}{37}\right) = \left(\frac{7919}{97}\right) = \left(\frac{62}{97}\right),$$

as $7919 \equiv 62 \bmod 97$. So far we know

$$\left(\frac{194}{7919}\right) = \left(\frac{62}{97}\right).$$

Now we apply the same procedure to the latter quadratic residue. We have

$$\left(\frac{62}{97}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{31}{97}\right).$$

By the second part of the theorem

$$\left(\frac{2}{97}\right) = (-1)^{(97^2-1)/8} = +1.$$

Next, by the first part,

$$\left(\frac{31}{97}\right) = (-1)^{(31-1)(97-1)/4}\left(\frac{97}{31}\right) = \left(\frac{97}{31}\right).$$

Since $97 \equiv 4 \bmod 31$, we have

$$\left(\frac{97}{31}\right) = \left(\frac{4}{31}\right) = \left(\frac{2}{31}\right)^2 = +1.$$

Putting everything together, we have

$$\left(\frac{194}{7919}\right) = +1.$$

6.3 An application of the Law of Quadratic Reciprocity

Let us return to Question 6.4. For $a \in \mathbb{Z}$, one can use the Law of Quadratic Reciprocity to characterize p such that

$$\left(\frac{a}{p}\right) = +1.$$

For example, let us study the case where $a = -3$. Suppose $p > 3$. We have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

Equation (6.3) gives

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Quadratic Reciprocity implies

$$\left(\frac{3}{p}\right) = (-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

Next,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$$

$$= \left(\frac{p}{3}\right) = \begin{cases} +1 & p \equiv 1 \mod 3; \\ -1 & p \equiv 2 \mod 3. \end{cases}$$

Let's think a moment about what just happened. We are trying to determine for what primes p, -3 is a quadratic residue modulo p. This is a question about quadratic residues modulo p: There are $(p-1)/2$ of these and that number grows with p, and that's somewhat of a moving target. The Law of Quadratic Reciprocity allows us to turn the problem around and transform it into a problem about quadratic residues

modulo 3. The beauty of this idea is that there is only one non-zero quadratic residue modulo 3, the congruence class of 1.

Next, following the argument leading to the proof of the infinitude of primes of the form $4k + 1$, we observe that if we multiply numbers of the form $3k + 1$ we will get another number of the form $3k + 1$:

$$(3m + 1)(3n + 1) = 3(3mn + m + n) + 1. \tag{6.4}$$

This is significant, as every prime number $p \neq 3$ either is of the form $3k + 1$ or of the form $3k + 2$. We can now prove the following theorem:

Theorem 6.9. *There are infinitely many primes of the form* $3k + 1$ *and infinitely many primes of the form* $3k + 2$.

Proof. The proof for $3k + 2$ is easy. Let $p_1, \ldots, p_m$ be a collection of odd primes of the form $3k + 2$. Set

$$M = 6p_1 \cdots p_m - 1.$$

The number M is not divisible by any of the p_i's, and Equation (6.4) means that not all of its prime factors can be of form $3k + 1$, because then M itself would be of the form $3k + 1$, which it is not. As a result, M must have a new prime factor of the form $3k + 2$, and this proves the second assertion of the theorem.

Next, we prove the first assertion. Again, let $p_1, \ldots, p_m$ be a collection of primes of the form $3k + 1$. Let

$$M = (2p_1 \cdots p_m)^2 + 3.$$

The number M is not divisible by 2, by 3, and by any of the p_i's. But no prime factor of M can be of the form $3k + 2$, because if $q \mid M$, then the equation $n^2 \equiv -3 \bmod q$ will have a solution in n, namely $n = 2p_1 \ldots p_m$. This means M must only consist of primes of the form $3k + 1$, and we have found new primes not among the p_i's. □

So far we have proved that each of the arithmetic progressions $2k + 1$ (Euclid!), $3k + 1, 3k + 2, 4k + 1$, and $4k + 3$ contains infinitely many primes. As we mentioned in the Notes to Chapter 5, a general theorem of Dirichlet, Theorem 5.11, provides a unifying picture for all of these results.

Exercises

6.1 Suppose we have a non-constant polynomial $f(x) \in \mathbb{Z}[x]$. Show that the set of prime numbers p such that $p \mid f(n)$ for some n is infinite.

6.2 Show for every non-constant polynomial $f(x) \in \mathbb{Z}[x]$ there are infinitely many values of n for which $f(n)$ is not prime.

6.3 Show that there are infinitely many primes of the form

a. $8k + 1$;
b. $8k + 3$;
c. $5k + 4$;
d. $12k + 1$;
e. $12k + 5$;
f. $12k + 7$;
g. $12k + 11$.

6.4 Compute the following Legendre symbols:

a. $(13/29)$;
b. $(67/193)$;
c. $(30/103)$;
d. $(62/569)$.

6.5 Give a group-theoretic interpretation for the Legendre symbol.
6.6 Suppose p is an odd prime, and $p \nmid a$. Show that the congruence $ax^2 + bx + c \equiv 0 \bmod p$ is solvable if and only if $u^2 \equiv b^2 - 4ac \bmod p$ is solvable.
6.7 Give a characterization for all primes p for which the equation $x^2 + 2x + 3 \equiv 0 \bmod p$ is solvable.
6.8 Determine all primes p that satisfy $(7/p) = +1$.
6.9 Prove that a prime p is of the form $x^2 - 2y^2$ if and only if $p = 2$ or $p \equiv \pm 1 \bmod 8$.
6.10 Prove if $(n/p) = -1$, then

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv 0 \mod p.$$

6.11 Determine the product of all quadratic residues modulo p.
6.12 Verify the identity

$$x^8 - 16 = (x^2 - 2)(x^2 + 2)((x - 1)^2 + 1)((x + 1)^2 + 1).$$

Use the identity to determine the number of solutions of

$$x^8 \equiv 16 \mod p.$$

6.13 Determine the number of solutions of the congruence

$$x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \mod p.$$

6.14 Show that if $p \mid n^4 - n^2 + 1$ for some $n \in \mathbb{Z}$, then $p \equiv 1 \bmod 12$.
6.15 Compute $\sum_{r=1}^{p-2} (r(r + 1)/p)$.
6.16 Let $p > 2$ be prime. Determine the number of $1 \leq n \leq p - 2$ such that n and $n + 1$ are both quadratic residues modulo p. To do this, consider

$$\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right).$$

6.17 Show that if n is not a perfect square, there are infinitely many primes p such that $(n/p) = -1$.

6.18 (✠) We saw in Exercise 2.60 that $p = 2^{17} - 1$ is prime. Compute the quadratic residue symbols (q/p) for q every prime less than 20.

6.19 Prove that there are arbitrarily long non-constant arithmetic progressions such that every two terms of the arithmetic progression are relatively prime.

6.20 Let $k \in \mathbb{N}$. Show that there are integers a, b such that for all $j \in \mathbb{N}$ the number of divisors of $a + bj$ is divisible by k.

6.21 Fix a natural number l. Assuming Theorem 5.11 prove every arithmetic progression $a + bk$, $k \geq 0$, with $\gcd(a, b) = 1$, contains infinitely many terms which are products of l distinct primes.

6.22 The goal of this exercise is to show that if $n \in \mathbb{N}$, then there are infinitely many primes of the form $nk + 1$.

a. Show that for each $d \in \mathbb{N}$ there is a monic polynomial $\Phi_d(x) \in \mathbb{Z}[x]$, called the *d-th cyclotomic polynomial*, such that

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

b. Show that $\Phi_1(0) = -1$ and for $d > 1$, $\Phi_d(0) = 1$.

c. (✠) Find the first 100 or so cyclotomic polynomials. Pay close attention to the coefficients of the polynomials.

d. Suppose $n > 1$ and $a \in \mathbb{Z}$, and let p be a prime divisor of $\Phi_n(a)$. Then show that $\gcd(a, p) = 1$, and if $h = o_p(a)$, $h \mid n$. Furthermore:
- if $h < n$, then

$$a^n - 1 \equiv (a + p)^n - 1 \equiv 0 \mod p^2;$$

- if $h < n$, then $p \mid n$;
- if $p \nmid n$, then $h = n$ and $p \equiv 1 \bmod n$.

e. Conclude there are infinitely many primes of the form $nk + 1$.

Notes

Infinitude of Prime Numbers in The Elements

To get a feel for Euclid's style of writing, let us state Euclid's First Theorem, Lemma 2.18:

Theorem 6.10 (Elements, Book VII, Proposition 30). *If two numbers by multiplying one another make some number, and any prime number measures [divides] the product, it will also measure one of the original numbers.*

It may sound like a historical absurdity that Euclid never stated Theorem 2.19—in fact, this particular fact had to wait almost 2000 years to be put in writing by Gauss. However, any rigorous proof of Theorem 2.19 uses mathematical induction which as a tool was not available to Euclid. At any rate, Euclid used this theorem to prove the irrationality of $\sqrt{n}$ for n non-square, which may have been his original goal in writing the number theoretic parts of *The Elements*.

This is Euclid's original formulation of Theorem 6.2:

Theorem 6.11 (Elements, Book IX, Proposition 20). *Prime numbers are more than any assigned multitude of prime numbers.*

Here we will reproduce Euclid's original argument. Note that here Euclid illustrates the idea by working out the proof for a special case:

Let A, B, and C be the assigned prime numbers. I say that there are more prime numbers than A, B, and C.

Take the least number DE measured by A, B, and C. Add the unit DF to DE. Then EF is either prime or not.

First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C.

Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G. I say that G is not the same with any of the numbers A, B, and C. If possible, let it be so.

Now A, B, and C measure DE; therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd.

Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C.

Therefore, prime numbers are more than any assigned multitude of prime numbers.

At the time of this writing, the largest known prime number is $2^{77,232,917} - 1$ discovered in 2017. This number has 23, 249, 425 digits. For comparison, the number of atoms in the entire observable universe is a number which is supposed to have about 80 digits. The discovery of this largest prime was part of *The Great Internet Mersenne Prime Search* accessible through

https://www.mersenne.org/

Primality testing

The first *primality test* is due to Eratosthenes (276–194 BCE) who observed that a number n is prime if and only if it is not divisible by any primes up to $\sqrt{n}$; see Exercise 2.18. For n reasonably small this provides a quick way of determining the primality of a number n, but as n gets large this method becomes impractical fairly quickly. Ideally one would like to be able to find a way to tell the primality of a number n in a number of steps that grows like a polynomial in the number of digits of n, and Eratosthenes' algorithm fails this expectation fairly miserably. Such an algorithm was not available until 2004 when the now-famous paper by M. Agrawal, N. Kayal, and N. Saxena [58] came out.

The algorithm presented in this paper is known as the AKS algorithm. Before AKS what was available in literature was an array of probabilistic algorithms, and some of these work quite well. A favorite example is the Miller–Rabin test [53, §6.3] which is based on Fermat's Little Theorem in elementary number theory. The Miller–Rabin test is extremely quick, but the trouble is that it gives *false positives*, in that some composite numbers are marked as primes.

A closely related problem we currently do not know how to solve, which is mentioned in the Notes of Chapter 2, is to factorize a large number as a product of its prime factors with reasonable efficiency. The solution of this problem would have far reaching consequences in terms of cryptography and internet security.

Twin Prime Conjecture

The following conjecture is considered very difficult:

Conjecture 6.12 (de Polignac, 1849). For every even natural number h, there are infinitely many prime numbers p such that $p + h$ is prime.

The case $h = 2$ is known as the *Twin Prime Conjecture* which at the time of this writing is still open. In 1915 Viggo Brun attempted to prove the Twin Prime Conjecture by proving that

$$\sum_{p,\, p+2 \text{ prime}} \frac{1}{p} \tag{6.5}$$

diverges. This idea goes back to Euler who proved the infinitude of prime numbers by showing that the series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

diverges. However, surprisingly, Brun proved that the series (6.5) is convergent! Even more surprisingly, the proof was fairly elementary; see Exercise 9.2.7 of [35] and the exercises leading up to it for a presentation of the argument. The theory of *sieves*

that Brun used in his proof has now become a powerful tool in number theory. The next major breakthrough, again involving the theory of sieves, was achieved in 1973 by Jingrun Chen [65] who showed that there are infinitely many primes p such that $p + 2$ is the product of at most two primes. In the same paper Chen also proved an approximation to Goldbach's conjecture; Chen proved every even number is the sum of a prime and a product of at most two primes. In 2005, Goldston, Pintz, and Yıldırım [76] proved a truly remarkable theorem. To state their theorem we will define a piece of notation. For a prime number p, let p_{next} be the smallest prime number larger than p. Using this notation, the Twin Prime Conjecture would assert the existence of infinitely many primes p such that $p_{\text{next}} - p = 2$. Goldston, Pintz, and Yıldırım used the theory of sieves in an ingenious way to prove

$$\liminf_{p\to\infty} \frac{p_{\text{next}} - p}{\log p} = 0.$$

It is clear that de Polignac's conjecture for any h would imply this result, but knowing this result would not give any information about de Polignac's conjecture. The spectacular work of Yitang Zhang in 2013, building on the techniques of Goldston, Pintz, and Yıldırım, changed the landscape overnight. Zhang [112] showed that there are infinitely many primes p such that

$$p_{\text{next}} - p < 7 \times 10^7.$$

This was a major achievement in that it showed the difference between consecutive primes was bounded by a uniform bound. In the last few years the bound of 7×10^7 has been substantially improved by Maynard [85] and the Polymath Project [91]. At the time of this writing we know by [91] that there are infinitely many primes p such that

$$p_{\text{next}} - p \leq 246.$$

At this time it is not clear how to reduce the bound 246, and this might require a new idea. The same paper proves that there are infinitely many primes p such that

$$(p_{\text{next}})_{\text{next}} - p \leq 38130.$$

It would also be of great interest to improve this bound, but, again, this might require an entirely new idea.