

Elementary Prime Number Theory, I

Prime numbers are more than any assigned multitude of
prime numbers. – Euclid

No prime minister is a prime number – A. Plantinga

1. Introduction

Recall that a natural number larger than 1 is called *prime* if its only positive divisors are 1 and itself, and *composite* otherwise. The sequence of primes begins

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...

Few topics in number theory attract more attention, popular or professional, than the theory of prime numbers. It is not hard to see why; the study of the distribution of the primes possesses in abundance the very features that draw so many of us to mathematics in the first place: intrinsic beauty, accessible points of entry, and a lingering sense of mystery embodied in numerous unpretentious but infuriatingly obstinate open problems.

Put

$$\pi(x) := \#\{p \leq x : p \text{ prime}\}.$$

Prime number theory begins with the following famous theorem from antiquity:

Theorem 1.1. *There are infinitely many primes, i.e., $\pi(x) \rightarrow \infty$ as $x \rightarrow \infty$.*

The first half of this chapter is a survey of the many proofs that have been given for Theorem 1.1. The second half of this chapter is devoted to the theme of prime-producing formulas and the occurrence of primes in various natural sequences.

2. Euclid and his imitators

We begin with the classic proof from Euclid's *Elements* (circa 300 BC):

Proof. Suppose that p_1, p_2, \dots, p_k is any finite list of primes. Let P denote the product of the p_i and consider the integer $P+1$. Since $P+1 \equiv 1 \pmod{p_i}$ for each $1 \leq i \leq k$, none of the p_i divide $P+1$. But since $P+1 > 1$, it must have some prime divisor p . It follows that there is always a prime missing from any finite list, or, as Euclid put it, "prime numbers are more than any assigned multitude of primes." \square

There are many trivial variants; for instance, we can easily show that for every integer m there is a prime $p > m$ by taking p to be any prime divisor of $m! + 1$.

In this section we collect several Euclid-style proofs for Theorem 1.1: all of these start with a finite list of primes and then produce an integer > 1 that is coprime to every prime on the list. Stieltjes's proof is typical:

Stieltjes's proof, 1890. Suppose that p_1, \dots, p_k is a finite list of distinct primes with product P and let $P = AB$ be any decomposition of P into two positive factors. Suppose that p is one of the p_i . Then $p \mid AB$, so that either $p \mid A$ or $p \mid B$. If p divides both A and B , then p^2 divides P , which is false. Consequently, p divides exactly one of A and B . It follows that $p \nmid A+B$. So $A+B$ is divisible by none of the p_i ; but as $A+B \geq 2$, it has some prime divisor. So again we have discovered a prime not on our original list. \square

Euler's second proof (published posthumously). This proof is based on the multiplicativity of the Euler totient function: Let p_1, \dots, p_k be a list of distinct primes with product P . By said multiplicativity,

$$\varphi(P) = \prod_{i=1}^k (p_i - 1) \geq 2^{k-1} \geq 2,$$

provided that our list contains at least two primes (as we may assume). It follows that there is an integer in the interval $[2, P]$ that is coprime to P ; but such an integer has a prime factor distinct from all of the p_i . \square

Proof of Braun (1897), Métrod (1917). Let p_1, \dots, p_k be a list of $k \geq 2$ distinct primes and let $P = p_1 p_2 \cdots p_k$. Consider the integer

$$N := P/p_1 + P/p_2 + \cdots + P/p_k.$$

For each $1 \leq i \leq k$, we have

$$N \equiv P/p_i = \prod_{j \neq i} p_j \not\equiv 0 \pmod{p_i},$$

so that N is divisible by none of the p_i . But $N \geq 2$, and so it must possess a prime factor not on our list. \square

3. Coprime integer sequences

Suppose we know an infinite sequence of pairwise relatively prime positive integers

$$2 \leq n_1 < n_2 < \cdots .$$

Then we may define a sequence of primes p_i by selecting arbitrarily a prime divisor of the corresponding n_i ; the terms of this sequence are pairwise distinct because the n_i are pairwise coprime.

If we can exhibit such a sequence of n_i without invoking the infinitude of the primes, then we have a further proof of Theorem 1.1. An argument of this nature was given by Goldbach:

Proof (Goldbach). Let $n_1 = 3$, and for $i > 1$ inductively define

$$n_i = 2 + \prod_{1 \leq j < i} n_j.$$

The following assertions are all easily verified in succession:

- (i) Each n_i is odd.
- (ii) When $j > i$, we have $n_j \equiv 2 \pmod{n_i}$.
- (iii) We have $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Theorem 1.1 now follows from the above remarks. \square

A straightforward induction shows that

$$(1.1) \quad n_i = 2^{2^{i-1}} + 1,$$

and this is how Goldbach presented the proof.

Before proceeding, we pause to note that the above proof implies more than simply the infinitude of the primes. First, it gives us an upper bound for the n th prime: $2^{2^{n-1}} + 1$; this translates into a lower bound of the shape

$$\pi(x) \gg \log \log x \quad (x \rightarrow \infty).$$

Second, it may be used to prove that certain arithmetic progressions contain infinitely many primes. To see this, suppose that $p \mid n_i$ and note that by (1.1), we have

$$2^{2^{i-1}} \equiv -1 \pmod{p}, \quad \text{so that} \quad 2^{2^i} \equiv (2^{2^{i-1}})^2 \equiv 1 \pmod{p}.$$

Hence the order of 2 modulo p is precisely 2^i . Thus $2^i \mid (\mathbf{Z}/p\mathbf{Z})^\times = p - 1$, so that $p \equiv 1 \pmod{2^i}$. As a consequence, for any fixed k , there are infinitely many primes $p \equiv 1 \pmod{2^k}$: choose a prime p_i dividing n_i for each $i \geq k$. In §9.1 we will prove the more general result that for each $m \geq 1$, there are infinitely many primes $p \equiv 1 \pmod{m}$.

A related method of proving the infinitude of the primes is as follows: Let $a_1 < a_2 < a_3 < \dots$ be a sequence of positive integers with the property that

$$\gcd(i, j) = 1 \implies \gcd(a_i, a_j) = 1.$$

Moreover, suppose that for some prime p , the integer a_p has at least two distinct prime divisors. Then if p_1, \dots, p_k were a list of all the primes, the integer

$$a_{p_1} a_{p_2} \cdots a_{p_k}$$

would possess at least $k + 1$ prime factors: indeed, each factor exceeds 1, the factors are pairwise relatively prime, and one of the factors is divisible by two distinct primes. So there are $k + 1 > k$ primes, a contradiction.

It remains to construct such a sequence. We leave to the reader the easy exercise of showing that $a_n = 2^n - 1$ has the desired properties (note that $a_{11} = 23 \cdot 89$). A similar proof taking instead a_n as the n th Fibonacci number was given by M. Wunderlich [Wun65] and was abstracted much as above by Hemminger .

Saidak [Sai06] has recently given a very simple argument making use of coprimality. Start with a natural number $n > 1$. Because n and $n + 1$ are coprime, the number $N_2 := n(n + 1)$ must have at least two distinct prime factors. By the same reasoning,

$$N_3 := N_2(N_2 + 1) = n(n + 1)(n(n + 1) + 1)$$

must have at least three distinct prime factors. In general, having constructed N_j with at least j different prime factors, the number $N_{j+1} := N_j(N_j + 1)$ must have at least $j + 1$.

4. The Euler-Riemann zeta function

For complex numbers s with real part greater than 1, define the zeta function by putting

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

(The condition that $\Re(s) > 1$ guarantees convergence of the series.) In the analytic approach to prime number theory, this function occupies a central position. Because of this text's emphasis on elementary methods, the zeta function will not play a large role for us, but it should be stressed that in

many of the deeper investigations into the distribution of primes, the zeta function is an indispensable tool.

Riemann introduced the study of $\zeta(s)$ as a function of a complex variable in an 1859 memoir on the distribution of primes [Rie59]. But the connection between the zeta function and prime number theory goes back earlier. Over a hundred years prior to Riemann's study, Euler had looked at the same series for real s and had shown that [Eul37, Theorema 8]

$$(1.2) \quad \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}} \quad (s > 1).$$

This is often called an analytic statement of unique factorization. To see why, notice that formally (i.e., disregarding matters of convergence)

$$\prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where a_n counts the number of factorizations of n into prime powers. Thus unique factorization, the statement that $a_n = 1$ for all n , is equivalent to the statement that (1.2) holds as a formal product of Dirichlet series.¹ This, in turn, is equivalent to the validity of (1.2) for all real $s > 1$ (or even a sequence of s tending to ∞) by a standard result in the theory of Dirichlet series (see, e.g., [Apo76, Theorem 11.3]).

Euler's product expansion of the zeta function is the first example of what is now called an *Euler factorization*. We now prove (following [Hua82]) a theorem giving general conditions for the validity of such factorizations.

Theorem 1.2 (Euler factorizations). *Let f be a multiplicative function. Then*

$$(1.3) \quad \sum_{n=1}^{\infty} f(n) = \prod_p \left(1 + f(p) + f(p^2) + \cdots \right)$$

if either of the following two conditions holds:

- (i) $\sum_{n=1}^{\infty} |f(n)|$ converges.
- (ii) $\prod_p (1 + |f(p)| + |f(p^2)| + \cdots)$ converges.

Remark. Without imposing a condition such as (i) or (ii), it is possible for either the series or the product in (1.3) to converge while the other diverges, or for both to converge without being equal. See [Win43, §15] for explicit examples.

¹Here a *Dirichlet series* is a series of the form $F(s) = \sum_{n=1}^{\infty} c_n/n^s$, where each c_n is a complex number.

If f is not merely multiplicative but completely multiplicative, then the factors in (1.3) form a geometric series whose convergence is implied by either of the above conditions. Thus we have the following consequence:

Corollary 1.3. *Let f be a completely multiplicative function. Then*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1 - f(p)}$$

subject to either of the two convergence criteria of Theorem 1.2.

The factorization (1.2) of the zeta function is immediate from this corollary: One takes $f(n) = 1/n^s$ and observes that for $s > 1$, condition (i) holds (for example) by the integral test.

Proof of Theorem 1.2. Suppose that condition (i) holds and set $S_0 := \sum_{n=1}^{\infty} |f(n)|$. For each prime p , the series $\sum_{k=0}^{\infty} f(p^k)$ converges absolutely, since $\sum_{k=0}^{\infty} |f(p^k)| \leq S_0$. Therefore

$$P(x) = \prod_{p \leq x} \left(1 + f(p) + f(p^2) + \cdots \right)$$

is a finite product of absolutely convergent series. It follows that

$$P(x) = \sum_{n: p|n \Rightarrow p \leq x} f(n).$$

If we now set $S = \sum_{n=1}^{\infty} f(n)$ (which converges absolutely), we have

$$S - P(x) = \sum_{n: p|n \text{ for some } p > x} f(n),$$

which shows

$$|S - P(x)| \leq \sum_{n > x} |f(n)| \rightarrow 0$$

as $x \rightarrow \infty$. Thus $P(x) \rightarrow S$ as $x \rightarrow \infty$, which is the assertion of (1.3).

Now suppose that (ii) holds. We shall show that (i) holds as well, so that the theorem follows from what we have just done. To see this, let

$$P_0 = \prod_p \left(1 + |f(p)| + |f(p^2)| + \cdots \right),$$

and let

$$\begin{aligned} P_0(x) &:= \prod_{p \leq x} \left(1 + |f(p)| + |f(p^2)| + \cdots \right) \\ &= \sum_{n: p|n \Rightarrow p \leq x} |f(n)| \geq \sum_{n \leq x} |f(n)|. \end{aligned}$$

Since $P_0(x) \leq P_0$ for all x , the partial sums $\sum_{n \leq x} |f(n)|$ form a bounded increasing sequence. Thus $\sum |f(n)|$ converges, proving (i). \square

We can now present Euler's first proof of the infinitude of the primes.

Euler's first proof of Theorem 1.1. Let f be defined by $f(n) = 1/n$ for every n . Assuming that there are only finitely many primes, condition (ii) of Theorem (1.3) is trivially satisfied, as the product in question only has finitely many terms. It follows that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) < \infty,$$

in contradiction with the well-known divergence of the harmonic series. \square

As pointed out by Euler, this proof gives a much stronger result than that asserted in Theorem 1.1.

Theorem 1.4. *The series $\sum \frac{1}{p}$ diverges, where the sum extends over all primes p .*

Proof. Suppose not and let $C = \sum 1/p$. As in the last proof, we take $f(n) = 1/n$ and apply Theorem 1.2. Let us check that condition (ii) of that theorem holds here. First, notice that

$$\prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq x} \left(1 + \frac{1}{p-1} \right) \leq \prod_{p \leq x} \left(1 + \frac{2}{p} \right).$$

Now recall that $e^t \geq 1 + t$ for every nonnegative t ; this is clear from truncating the Taylor expansion $e^t = 1 + t + t^2/2! + \dots$. It follows that

$$\prod_{p \leq x} \left(1 + \frac{2}{p} \right) \leq \prod_{p \leq x} e^{2/p} = \exp \left(\sum_{p \leq x} 2/p \right) \leq \exp(2C).$$

Consequently, the partial products

$$\prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right)$$

form a bounded, increasing sequence, which shows that we have condition (ii). We conclude that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \frac{1}{1 - \frac{1}{p}} \leq \exp(2C),$$

a contradiction. \square

Tweaking this argument, it is possible to derive an explicit lower bound on the partial sums $\sum_{p \leq x} 1/p$: Note that for $x \geq 2$,

$$(1.4) \quad \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \sum_{n: p|n \Rightarrow p \leq x} \frac{1}{n} \geq \sum_{n \leq x} \frac{1}{n} \geq \log x.$$

From the upper bound $(1 - 1/p)^{-1} = (1 + 1/(p-1)) \leq \exp((p-1)^{-1})$, we deduce (taking the logarithm of (1.4)) that $\sum_{p \leq x} (p-1)^{-1} \geq \log \log x$. To derive a lower bound for $\sum_{p \leq x} 1/p$ from this, note that

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \sum_{p \leq x} \frac{1}{p-1} - \sum_{p \leq x} \left(\frac{1}{p-1} - \frac{1}{p} \right) \\ (1.5) \quad &\geq \sum_{p \leq x} \frac{1}{p-1} - \sum_{n \geq 2} \left(\frac{1}{n-1} - \frac{1}{n} \right) = \left(\sum_{p \leq x} \frac{1}{p-1} \right) - 1 \geq \log \log x - 1. \end{aligned}$$

The next two proofs also make use of the zeta function and its Euler factorization, but in a decidedly different manner.

Proof of J. Hacks. We need the well-known result, also due to Euler, that $\zeta(2) = \pi^2/6$; a proof is sketched in Exercise 4 (for alternative arguments see [AZ04, Chapter 7], [Cha02]). Plugging $s = 2$ into the Euler factorization (1.2) we obtain

$$\frac{\pi^2}{6} = \zeta(2) = \prod_p \frac{1}{1 - \frac{1}{p^2}}.$$

If there are only finitely many primes, then the product appearing here is a finite product of rational numbers, so that $\pi^2/6$ must also be a rational number. But this is impossible, since π is well-known to be a *transcendental number*, i.e., not the root of any nonzero polynomial with rational coefficients. (A weaker result, which suffices for the current argument, is the subject of Exercise 5.) \square

One can give a similar argument avoiding irrationality considerations:

Proof. We use not only that $\zeta(2) = \pi^2/6$ but also that $\zeta(4) = \pi^4/90$. (Again see Exercise 4.) Thus $\zeta(2)^2/\zeta(4) = 5/2$. The Euler factorization (1.2) implies that

$$\frac{5}{2} = \frac{\zeta(2)^2}{\zeta(4)} = \prod_p (1 - p^{-4})(1 - p^{-2})^{-2} = \prod_p \frac{p^4 - 1}{p^4} \frac{p^4}{(p^2 - 1)^2} = \prod_p \frac{p^2 + 1}{p^2 - 1},$$

so that

$$\frac{5}{2} = \frac{5}{3} \cdot \frac{10}{8} \cdot \frac{26}{24} \cdots.$$

If there are only finitely many primes, then the product on the right-hand side is a finite one and can be written as M/N , where $M = 5 \cdot 10 \cdot 26 \cdots$ and $N = 3 \cdot 8 \cdot 24 \cdots$. Then $M/N = 5/2$, so $2M = 5N$. Since $3 \mid N$, it must be that $3 \mid M$. But this cannot be: M is a product of numbers of the form $k^2 + 1$, and no such number is a multiple of 3. \square

Wagstaff has asked whether one can give a more elementary proof that $5/2 = \prod_p \frac{p^2+1}{p^2-1}$. The discussion of this (open) question in [Guy04, B48] was the motivation for the preceding proof of Theorem 1.1.

5. Squarefree and smooth numbers

Recall that a natural number n is said to be *squarefree* if it is not divisible by the square of any integer larger than 1. The fundamental theorem of arithmetic shows that there is a bijection

$$\{\text{finite subsets of the primes}\} \longleftrightarrow \{\text{squarefree positive integers}\},$$

given by sending

$$S \longmapsto \prod_{p \in S} p.$$

So to prove the infinitude of the primes, it suffices to prove that there are infinitely many positive squarefree integers.

J. Perott's proof, 1881. We sieve out the non-squarefree integers from $1, \dots, N$ by removing those divisible by 1^2 , then those divisible by 2^2 , etc. The number of removed integers is bounded above by

$$\sum_{k=2}^{\infty} \lfloor N/k^2 \rfloor \leq N \sum_{k=2}^{\infty} k^{-2} = N(\zeta(2) - 1),$$

so that the number of squarefree integers up to N , say $A(N)$, satisfies

$$(1.6) \quad A(N) \geq N - N(\zeta(2) - 1) = N(2 - \zeta(2)).$$

At this point Perott uses the evaluation $\zeta(2) = \pi^2/6$. However, it is simpler to proceed as follows: Since t^{-2} is a decreasing function of t on the positive real axis,

$$\zeta(2) = 1 + \sum_{n=2}^{\infty} \frac{1}{n^2} < 1 + \sum_{n=1}^{\infty} \int_n^{n+1} \frac{dt}{t^2} = 1 + \int_1^{\infty} \frac{dt}{t^2} = 2.$$

Referring back to (1.6), we see that $A(N)/N$ is bounded below by a positive constant. In particular, it must be that $A(N) \rightarrow \infty$ as $N \rightarrow \infty$. \square

Remark. As observed by Dressler [Dre75], Perott's argument also yields a lower bound on $\pi(N)$. Note that since every squarefree number $\leq N$ is a product of some subset of the $\pi(N)$ primes up to N , we have $2^{\pi(N)} \geq A(N)$. The argument above establishes that $A(N) \geq cN$ for $c = 2 - \zeta(2) > 0$, and so $\pi(N) \geq \log N/\log 2 + O(1)$.

For the next proof we need the following simple lemma:

Lemma 1.5. *Every natural number n can be written in the form rs^2 , where r and s are natural numbers.*

Proof. Choose the positive integer s so that s^2 is the largest perfect square dividing n , and put $r = n/s^2$. We claim that r is squarefree. Otherwise $p^2 \mid r$ for some prime p . But then $(ps)^2 \mid n$, contrary to the choice of s . \square

Erdős's proof of Theorem 1.1. Let N be a positive integer. There are at most \sqrt{N} squares not exceeding N and at most $2^{\pi(N)}$ squarefree integers below this bound. So Lemma 1.5 implies that

$$2^{\pi(N)}\sqrt{N} \geq N.$$

Dividing by \sqrt{N} and taking logarithms yields the lower bound $\pi(N) \geq \log N / \log 4$. \square

A modification of this argument leads to another proof that $\sum \frac{1}{p}$ diverges:

Erdős's proof of Theorem 1.4. Suppose that $\sum 1/p$ converges. Then we can choose an M for which

$$(1.7) \quad \sum_{p>M} \frac{1}{p} < \frac{1}{2}.$$

Keep this M fixed.

Let N be an arbitrary natural number. The estimate (1.7) implies that most integers up to N factor completely over the primes not exceeding M . Indeed, the number of integers not exceeding N that have a prime factor $p > M$ is bounded above by

$$\sum_{M < p \leq N} \left\lfloor \frac{N}{p} \right\rfloor \leq N \sum_{p>M} \frac{1}{p} < N/2,$$

so that more than $N/2$ of the natural numbers not exceeding N are divisible only by primes $p \leq M$.

We now show that there are too few integers divisible only by primes $p \leq M$ for this to be possible. There are at most \sqrt{N} squares not exceeding N and at most $C := 2^{\pi(M)}$ squarefree numbers composed only of primes not exceeding M . Thus there are at most $C\sqrt{N}$ natural numbers $\leq N$ having all their prime factors $\leq M$. But $C\sqrt{N} < N/2$ once $N > 4C^2$. \square

In the last argument we needed an estimate for the number of integers up to a given point with only small prime factors. This motivates the following definition: Call a natural number y -smooth if all of its prime factors are bounded by y . We let $\Psi(x, y)$ denote the number of y -smooth numbers not exceeding x ; i.e.,

$$(1.8) \quad \Psi(x, y) := \#\{n \leq x : p \mid n \Rightarrow p \leq y\}.$$

Smooth numbers are important auxiliary tools in many number-theoretic investigations, and so there has been quite a bit of work on estimating the

size of $\Psi(x, y)$ in various ranges of x and y . (For a survey of both the applications and the estimates, see [Gra08b].) A trivial estimate yields an easy proof of Theorem 1.1.

Lemma 1.6. *For $x \geq 1$ and $y \geq 2$, we have*

$$\Psi(x, y) \leq \left(1 + \frac{\log x}{\log 2}\right)^{\pi(y)}.$$

Proof. Let $k = \pi(y)$. By the fundamental theorem of arithmetic, $\Psi(x, y)$ is the number of k -tuples of nonnegative integers e_1, \dots, e_k with

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \leq x.$$

This inequality requires $p_i^{e_i} \leq x$, so that

$$e_i \leq \log x / \log p_i \leq \log x / \log 2,$$

so that there are at most $1 + \lceil \log x / \log 2 \rceil$ possibilities for each e_i . \square

Since every positive integer not exceeding N is a (possibly empty) product of primes not exceeding N ,

$$N = \Psi(N, N) \leq (1 + \log N / \log 2)^{\pi(N)}.$$

It follows that

$$\pi(N) \geq \frac{\log N}{\log(1 + \log N / \log 2)}.$$

Taking some care to estimate the denominator, we obtain the lower bound

$$\pi(N) \geq (1 + o(1)) \frac{\log N}{\log \log N},$$

which tends to infinity. Similar proofs of Theorem 1.1 have been given by Thue (1897), Auric (1915), Schnirelmann [Sch40, pp. 44–45], Chernoff [Che65], and Rubinstein [Rub93]. See also Exercise 16.

6. Sledgehammers!

In the spirit of the saying “everything simple can be made complicated with enough hard work,” we finish off the first half of this chapter with two proofs of Theorem 1.1 that dip into the tool chest of higher mathematics.

The following ‘topological proof’ is due to Furstenberg ([Fur55]):

Proof. We put a topology on \mathbf{Z} by taking as a basis for the open sets all arithmetic progressions, infinite in both directions. (This is permissible since the intersection of two such progressions is either empty or is itself an arithmetic progression.) Then each arithmetic progression is both open and closed: it is open by choice of the basis, and it is closed since its complement is the union of the other arithmetic progressions with the same common

difference. For each prime p , let $A_p = p\mathbf{Z}$, and define $A := \cup_p A_p$. The set $\{-1, 1\} = \mathbf{Z} \setminus A$ is not open. (Indeed, every open set is either empty or contains an arithmetic progression, so infinite.) It follows that A is not closed. On the other hand, if there are only finitely many primes then A is a finite union of closed sets, and so *is* closed. \square

Our next proof, due to L. Washington (and taken from [Rib96]) uses the machinery of commutative algebra. Recall that a *Dedekind domain* is an integral domain R with the following three properties:

- (i) R is *Noetherian*: if $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an ascending chain of ideals of R , then there is an n for which

$$I_n = I_{n+1} = I_{n+2} = \cdots .$$

- (ii) R is *integrally closed*: if K denotes the fraction field of R and $\alpha \in K$ is the root of a monic polynomial with coefficients in R , then in fact $\alpha \in R$.

- (iii) Every nonzero prime ideal of R is a maximal ideal.

Proof. We use the theorem that a Dedekind domain with finitely many nonzero prime ideals is a principal ideal domain (see, e.g., [Lor96, Proposition III.2.12]) and so is also a unique factorization domain. The ring of integers $\mathfrak{O}\mathfrak{B}_K$ of a number field K is always a Dedekind domain; consequently, if K does not possess unique factorization, then $\mathfrak{O}\mathfrak{B}_K$ has infinitely many nonzero prime ideals. Each such prime ideal lies above a rational prime p , and for each prime p there are at most $[K : \mathbf{Q}]$ prime ideals lying above it. It follows that there are infinitely many primes p , provided that there is a single number field K for which $\mathfrak{O}\mathfrak{B}_K$ does not possess unique factorization. And there is: If $K = \mathbf{Q}(\sqrt{-5})$, then

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

is a well-known instance of the failure of unique factorization in $\mathfrak{O}\mathfrak{B}_K = \mathbf{Z}[\sqrt{-5}]$. \square

7. Prime-producing formulas

A mathematician is a conjurer who gives away his secrets. – J. H. Conway

Now that we know that there are infinitely many primes, the next question is: Where are they hiding? Or, to ask a question that has ensnared many who have flirted with number theory, is there a formula for producing primes? This line of inquiry, as natural as it seems, has not been very productive.

The following 1952 result of Sierpiński [Sie52] is representative of many in this subject. Let p_n denote the n th prime number. Define a real number ξ by putting

$$\xi := \sum_{n=1}^{\infty} p_n 10^{-2^n} = 0.0203000500000007000000000000011\dots$$

★ **Theorem 1.7.** *We have*

$$p_n = \lfloor 10^{2^n} \xi \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \xi \rfloor.$$

This is, in the literal sense, a formula for primes. But while it may have some aesthetic merit, it must be considered a complete failure from the standpoint of utility; determining the number ξ seems to require us to already know the sequence of primes. A similar criticism can be leveled against a result of Mills [Mil47], which asserts the existence of a real number $A > 1$ with the property that $\lfloor A^{3^n} \rfloor$ is prime for each natural number n .

A more surprising way of generating primes was proposed by J. H. Conway [Con87]. Consider the following list of 14 fractions:

| | | | | | | | | | | | | | |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|----------------|-----------------|-----------------|----------------|---------------|----------------|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| $\frac{17}{91}$ | $\frac{78}{85}$ | $\frac{19}{51}$ | $\frac{23}{38}$ | $\frac{29}{33}$ | $\frac{77}{29}$ | $\frac{95}{23}$ | $\frac{77}{19}$ | $\frac{1}{17}$ | $\frac{11}{13}$ | $\frac{13}{11}$ | $\frac{15}{2}$ | $\frac{1}{7}$ | $\frac{55}{1}$ |

Now run the following algorithm: Beginning with the number 2, look for the first (leftmost) fraction which can be multiplied by the current number to give an integer. Perform the multiplication and repeat. Whenever you reach a power of 2, output the exponent. The first several (19) steps of the algorithm are

$$2 \mapsto 15 \mapsto 825 \mapsto 725 \mapsto 1925 \mapsto 2275 \mapsto 425 \mapsto 390 \mapsto 330 \mapsto 290 \mapsto 770 \\ \mapsto 910 \mapsto 170 \mapsto 156 \mapsto 132 \mapsto 116 \mapsto 308 \mapsto 364 \mapsto 68 \mapsto 4 = 2^2,$$

and so the first output is 2. Fifty more steps yield

$$2^2 \mapsto 30 \mapsto 225 \mapsto 12375 \mapsto \dots \mapsto 232 \mapsto 616 \mapsto 728 \mapsto 136 \mapsto 8 = 2^3,$$

and so the second output is 3. After another 212 steps, we arrive at $32 = 2^5$, and so our third output is 5.

★ **Theorem 1.8** (Conway). *The sequence of outputs is exactly the sequence of primes in increasing order.*

This is rather striking; the sequence of primes, which seems random in so many ways, is the output of a deterministic algorithm involving 14 fractions. But perhaps this should not come as such a shock. Most anyone who has experimented with programming knows that the primes are the output of a deterministic algorithm: Test the numbers 2, 3, 4, ... successively for

primality, using (say) trial division for the individual tests. And actually, underneath the surface, this is exactly what is being done in Conway's algorithm. This sequence of 14 fractions encodes a simple computer program: The number n is tested for divisibility first by $d = n - 1$, then $d = n - 2$, etc; as soon as a divisor is found, n is incremented by 1 and the process is repeated. The game is rigged so that a power of 2 arises only when d reaches 1, i.e., when n is prime. Moreover, there is nothing special in Theorem 1.8 about the sequence of primes; an analogue of Theorem 1.8 can be proved for any recursive set. (Here a set of natural numbers S is called *recursive* if there is an algorithm for determining whether a natural number belongs to S .) We conclude that while Conway's result *is* genuinely surprising, the surprise is that one can simulate computer programs with lists of fractions, and is in no way specific to the prime numbers.

8. Euler's prime-producing polynomial

The prime-producing functions we have been considering up to now have all been rather complicated. In some sense this is necessary; one can show that any function which produces only primes cannot have too simple a form. We give only one early example of a result in this direction. (See [War30], [Rei43] for more theorems of this flavor.)

Theorem 1.9 (Goldbach). *If $F(T) \in \mathbf{Z}[T]$ is a nonconstant polynomial with positive leading coefficient, then $F(n)$ is composite for infinitely many natural numbers n .*

Proof. Suppose F is nonconstant but that $F(n)$ is prime for all $n \geq N_0$, where N_0 is a natural number. Let $p = F(N_0)$; then p divides $F(N_0 + kp)$ for every positive integer k . But since F has positive leading coefficient, $F(N_0 + kp) > p$ for every sufficiently large integer k , and so $F(N_0 + kp)$ is composite, contrary to the choice of N_0 . \square

Theorem 1.9 does not forbid the existence of polynomials F which assume prime values over impressively long stretches. And indeed these do exist; a famous example is due to Euler, who observed that if $f(T) = T^2 + T + 41$, then $f(n)$ is prime for all integers $0 \leq n < 40$.

It turns out that Euler's observation, rather than being an isolated curiosity, is intimately connected with the theory of imaginary quadratic fields. We will prove the following theorem:

Theorem 1.10. *Let $A \geq 2$, and set $D := 1 - 4A$. Then the following are equivalent:*

- (i) $n^2 + n + A$ is prime for all $0 \leq n < A - 1$,

- (ii) $n^2 + n + A$ is prime for all $0 \leq n \leq \frac{1}{2}\sqrt{\frac{|D|}{3}} - \frac{1}{2}$,
- (iii) the ring $\mathbf{Z}[(-1 + \sqrt{D})/2]$ is a unique factorization domain.

The equivalence (i) \Leftrightarrow (iii) is proved by Rabinowitsch in [Rab13], and is usually referred to as *Rabinowitsch's theorem*.

Remark. Since $n^2 + n + A = (n + 1/2)^2 + (4A - 1)/4$, (ii) can be rephrased as asserting that $(n + 1/2)^2 + |D|/4$ is prime for every integer n for which $|n + 1/2| \leq \frac{1}{2}\sqrt{\frac{|D|}{3}}$. We will use this observation in the proof of Theorem 1.10.

Cognoscenti will recognize that $\mathbf{Z}[(-1 + \sqrt{D})/2]$ is an order in the quadratic field $\mathbf{Q}(\sqrt{D})$. However, the proof of Theorem 1.10 presented here, due to Gyarmati (née Lanczi) [Lán65], [Gya83] and Zaupper [Zau83], requires neither the vocabulary of algebraic number theory nor the theory of ideals.

We begin the proof of Theorem 1.10 by observing that the bound on n in (ii) is always at least as strict as the bound on n in (i), which makes clear that (i) implies (ii). So it is enough to show that (ii) implies (iii) and that (iii) implies (i). To continue we need some preliminary results on the arithmetic of the rings $\mathbf{Z}[(-1 + \sqrt{D})/2]$. These will be familiar to students of algebraic number theory, but we include full proofs for the sake of completeness.

Let $A \geq 2$ be an integer, and fix a complex root η of $x^2 + x + A$, so that (for an appropriate choice of the square root) $\eta = (-1 + \sqrt{D})/2$. Since $\eta^2 = -\eta - A$, it follows that

$$\mathbf{Z}[\eta] = \mathbf{Z} + \mathbf{Z}\eta = \{x + y\eta : x, y \in \mathbf{Z}\}.$$

For $\alpha \in \mathbf{Z}[\eta]$, we denote its complex conjugate by $\bar{\alpha}$. Observe that $\bar{\eta} = -1 - \eta$; consequently, $\mathbf{Z}[\eta]$ is closed under complex-conjugation. We define the *norm* of the element $\alpha = x + y\eta \in \mathbf{Z}[\eta]$ by

$$\begin{aligned} \mathcal{N}(\alpha) &:= |\alpha|^2 \\ &= \alpha\bar{\alpha} = x^2 - xy + Ay^2. \end{aligned}$$

Notice that the norm of $\alpha \in \mathbf{Z}[\eta]$ is always an integer and is positive whenever $\alpha \neq 0$. Moreover, since the complex absolute value is multiplicative, it is immediate that

$$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta) \quad \text{for all } \alpha, \beta \in \mathbf{Z}[\eta].$$

We now recall the requisite definitions from ring theory: If $\alpha, \beta \in \mathbf{Z}[\eta]$, we say that α *divides* β if $\beta = \alpha\gamma$ for some $\gamma \in \mathbf{Z}[\eta]$. A nonzero element $\alpha \in \mathbf{Z}[\eta]$ is called a *unit* if α divides 1. A nonunit element $\alpha \in \mathbf{Z}[\eta]$ is *irreducible* if whenever $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbf{Z}[\eta]$, then either β is a unit or

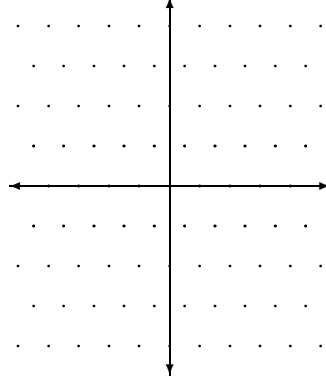


Figure 1. The lattice $\mathbf{Z} + \mathbf{Z}\eta$ sitting inside \mathbf{C} . Here $A = 2$ so that $D = -7$.

γ is a unit. Finally, $\pi \in \mathbf{Z}[\eta]$ is called *prime* if whenever π divides $\beta\gamma$ for $\beta, \gamma \in \mathbf{Z}[\eta]$, then either π divides β or π divides γ .

Lemma 1.11. *An element $\alpha \in \mathbf{Z}[\eta]$ is a unit precisely when $\mathcal{N}(\alpha) = 1$. The only units in $\mathbf{Z}[\eta]$ are ± 1 .*

Proof. If α is a unit, then $\mathcal{N}(\alpha) \cdot \mathcal{N}(\alpha^{-1}) = 1$. Moreover, both $\mathcal{N}(\alpha)$ and $\mathcal{N}(\alpha^{-1})$ are positive integers, so that $\mathcal{N}(\alpha) = \mathcal{N}(\alpha^{-1}) = 1$. Conversely, if $\mathcal{N}(\alpha) = 1$, then $\alpha\bar{\alpha} = 1$, and so α is a unit. Finally, notice that if $y \neq 0$, then

$$\mathcal{N}(x + y\eta) = x^2 - xy + Ay^2 = (x - y/2)^2 + \frac{1}{4}(4A - 1)y^2 \geq \frac{4A - 1}{4}y^2 > \frac{7}{4} > 1.$$

So $x + y\eta$ can be a unit only when $y = 0$. In this case we must have $\mathcal{N}(x) = x^2 = 1$, and this occurs exactly when $x = \pm 1$. \square

Lemma 1.12. *If α is a nonzero, nonunit element of $\mathbf{Z}[\eta]$, then α can be written as a product of irreducible elements of $\mathbf{Z}[\eta]$.*

Proof. If the claim fails, there is a nonzero, nonunit α of smallest norm for which it fails. Clearly α is not irreducible, and so we can write $\alpha = \beta\gamma$, where β and γ are nonzero nonunits. Hence $\mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\gamma)$. Since $\mathcal{N}(\beta)$ and $\mathcal{N}(\gamma)$ are each larger than 1, both $\mathcal{N}(\beta)$ and $\mathcal{N}(\gamma)$ must be smaller than $\mathcal{N}(\alpha)$. So by the choice of α , both β and γ factor as products of irreducibles, and thus α does as well. This contradicts the choice of α . \square

We can now prove one the two outstanding implications:

Proof that (iii) \Rightarrow (i). Let $\eta = (-1 + \sqrt{D})/2$. Suppose $0 \leq n < A - 1$. We have

$$(1.9) \quad n^2 + n + A = (n - \eta)(n - \bar{\eta}) = (n - \eta)(n + 1 + \eta).$$

Let p be a prime dividing $n^2 + n + A$. We claim that p is not irreducible in $\mathbf{Z}[\eta]$. Indeed, since $\mathbf{Z}[\eta]$ is a unique factorization domain by hypothesis, if p were irreducible then p would be prime. So from (1.9), we would have that p divides $n - \eta$ or $n + 1 + \eta$. But this is impossible, since neither $n/p - \eta/p$ nor $(n + 1)/p + \eta/p$ belongs to $\mathbf{Z}[\eta] = \mathbf{Z} + \mathbf{Z}\eta$.

Hence we can write $p = \alpha\beta$, where $\alpha, \beta \in \mathbf{Z}[\eta]$ and neither α nor β is a unit. Taking norms, we deduce that $p^2 = \mathcal{N}(p) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$. Since α and β are not units, must have $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = p$.

Write $\alpha = x + y\eta$ for integers x, y . Then $y \neq 0$ (since p is a rational prime), and so

$$p = N(\alpha) = x^2 - xy + Ay^2 = (x - y/2)^2 + (A - 1/4)y^2 \geq A - 1/4.$$

Thus (since p is an integer) $p \geq A$. Moreover, since $0 \leq n < A - 1$,

$$n^2 + n + A < (A - 1)^2 + (A - 1) + A = (A - 1)A + A = A^2.$$

This shows that every prime divisor of $n^2 + n + A$ exceeds its square root, so that $n^2 + n + A$ is prime. \square

The proof of the remaining implication requires one more preliminary result:

Lemma 1.13. *If π is an element of $\mathbf{Z}[\eta]$ whose norm is a rational prime p , then π is prime in $\mathbf{Z}[\eta]$.*

Proof. We claim that $\mathbf{Z}[\eta]/(\pi)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Since $\mathbf{Z}/p\mathbf{Z}$ is a field, this implies that π generates a prime ideal of $\mathbf{Z}[\eta]$, which in turn implies that π is prime. Let $\psi: \mathbf{Z} \rightarrow \mathbf{Z}[\eta]/(\pi)$ be the ring homomorphism defined by mapping n to $n \bmod \pi$. Since $p = \pi\bar{\pi} \equiv 0 \pmod{\pi}$, the kernel of ψ contains the ideal $p\mathbf{Z}$. Since $p\mathbf{Z}$ is a maximal ideal, either ψ is identically zero or the kernel of ψ is precisely $p\mathbf{Z}$. Since π is not a unit in $\mathbf{Z}[\eta]$, $\psi(1)$ is nonzero, and so the kernel of ψ is precisely $p\mathbf{Z}$. Hence $\mathbf{Z}/p\mathbf{Z}$ is isomorphic to the image of ψ . So the proof will be complete if we show that ψ is surjective.

Write $\pi = r + s\eta$ for integers r and s , and let $x + y\eta$ be an arbitrary element of $\mathbf{Z}[\eta]$. We can choose integers a and b for which

$$m := x + y\eta - \pi(a + b\eta) \in \mathbf{Z}.$$

Indeed, a short computation shows that this containment holds precisely when

$$b(r - s) + as = y,$$

which is a solvable linear Diophantine equation in a and b since $\gcd(r - s, s) = \gcd(r, s) = 1$. Then $m \equiv x + y\eta \pmod{\pi}$, and so $\psi(m) = x + y\eta \bmod \pi$. Since $x + y\eta$ was arbitrary, ψ is surjective as claimed. \square

Proof that (ii) \Rightarrow (iii). Suppose that $n^2 + n + A$ is prime for all

$$0 \leq n \leq \frac{1}{2} \sqrt{\frac{|D|}{3}} - \frac{1}{2}.$$

We are to prove that $\mathbf{Z}[\eta]$ possesses unique factorization. Suppose otherwise, and let α be a nonzero, nonunit of minimal norm with two distinct factorizations into irreducibles, say

$$\alpha = \pi_1 \cdots \pi_k = \rho_1 \cdots \rho_j.$$

(Here *distinct* means that either $k \neq j$, or that $k = j$ but there is no way to reorder the π_i so that each π_i is a unit multiple of ρ_i .) By the minimality of $\mathcal{N}(\alpha)$, it is easy to see that none of the irreducibles in the first factorization can be a unit multiple of an irreducible in the second factorization. Consequently, none of the irreducibles appearing in either factorization can be prime in $\mathbf{Z}[\eta]$.

We can assume that $\mathcal{N}(\pi_1) \leq \mathcal{N}(\rho_1)$. (If this does not hold initially, interchange the two factorizations.) For $\xi, \gamma \in \mathbf{Z}[\eta]$ still to be chosen, define

$$(1.10) \quad \alpha' := (\rho_1 \xi - \pi_1 \gamma) \rho_2 \cdots \rho_j.$$

Then

$$\begin{aligned} \alpha' &= \alpha \xi - \pi_1 \frac{\alpha}{\rho_1} \gamma \\ &= \pi_1 (\pi_2 \cdots \pi_k \xi - \rho_2 \cdots \rho_j \gamma). \end{aligned}$$

Factoring the parenthesized expression, we deduce that α' has a factorization into irreducibles where one of the irreducibles is π_1 . We will choose ξ and γ so that $\pi_1 \nmid \rho_1 \xi$. Then $\pi_1 \nmid \rho_1 \xi - \pi_1 \gamma$, and so we may deduce from (1.10) that α' has a factorization into irreducibles, none of which is a unit multiple of π_1 . So α' possesses two distinct factorizations into irreducibles. If further, γ and ξ satisfy

$$\mathcal{N}(\rho_1 \xi - \pi_1 \gamma) < \mathcal{N}(\rho_1),$$

then $\mathcal{N}(\alpha')$ is smaller than $\mathcal{N}(\alpha)$, and so we have a contradiction to our choice of α .

So it remains to show that it is possible to choose $\xi, \gamma \in \mathbf{Z}[\eta]$ with the following two properties:

$$(P1) \quad \pi_1 \nmid \rho_1 \xi,$$

$$(P2) \quad \mathcal{N}(\rho_1 \xi - \pi_1 \gamma) < \mathcal{N}(\rho_1), \text{ or equivalently, } \left| \xi - \frac{\pi_1}{\rho_1} \gamma \right| < 1.$$

Since $\mathcal{N}(\pi_1) \leq \mathcal{N}(\rho_1)$, the complex number π_1/ρ_1 lies on or inside the unit circle. Suppose first that π_1/ρ_1 lies outside the shaded region indicated in Figure 2. Then for either $\xi = 1$ or $\xi = -1$, we have

$$\left| \xi - \pi_1/\rho_1 \right| < 1.$$

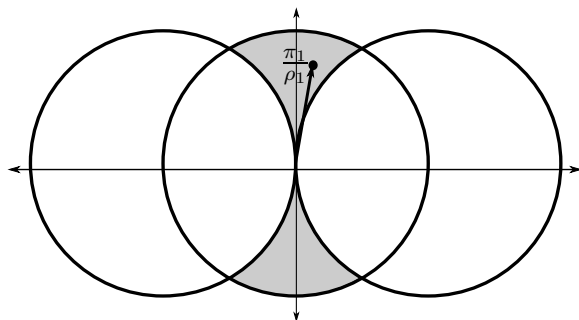


Figure 2. (Reproduced from [Zau83].)

Then (P1) and (P2) hold if we choose this value of ξ and take $\gamma = 1$. Note that $\pi_1 \nmid \pm\rho_1$, since otherwise π_1 and ρ_1 would be unit multiples of each other, which we have already argued is not the case.

So we may assume that π_1/ρ_1 lies within the shaded region. Let e_1 be the ray from the origin making an angle of 60° with the x -axis, and let e_2 be the ray from the origin making an angle of 120° with that axis. Then the ray e (say) from the origin through π_1/ρ_1 is contained within the 60° angle determined by e_1 and e_2 .² Let f be the horizontal line consisting of those complex numbers with imaginary part $\sqrt{|D|}/2$; thus f is the first horizontal line above the x -axis containing points of the lattice $\mathbf{Z} + \mathbf{Z}\eta$. Let μ be the complex number corresponding to the intersection of e and f . The angle determined by e_1 and e_2 cuts f in a segment of length $\sqrt{|D|/3} > 1$, and so there is a point of $\mathbf{Z} + \mathbf{Z}\eta$ on f within this angle. We choose such a point ξ for which the distance from ξ to μ is as small as possible. See Figure 3.

We claim that the distance from ξ to e is strictly smaller than $\sqrt{3}/2$. This is clear if both $\xi + 1$ and $\xi - 1$ fall within the angle determined by e_1 and e_2 , since in that case, the distance from ξ to μ must be at most $1/2$. So suppose that $\xi + 1$ falls outside this angle; the case when $\xi - 1$ falls outside is analogous. Then $\xi - 1$ must lie within the given angle. If now ξ is to the right of μ , then in order that ξ be at least as close to μ as $\xi - 1$, it must be that the distance from ξ to μ is at most $1/2$. So we can assume that ξ falls to the left of μ . This is the scenario depicted in Figure 3. In this case we use the following argument: Let ν represent the intersection of e_1 and f ; then the distance between ξ and ν is smaller than 1. Since e_1 makes an angle of 60° with f , elementary trigonometry shows that the distance from ξ to e_1 is strictly smaller than $\sqrt{3}/2$. But the perpendicular line segment from ξ to e_1 meets e . So the distance from ξ to e is also strictly smaller than $\sqrt{3}/2$.

²Here the *angle determined by e_1 and e_2* means the closed set of points between e_1 and e_2 .

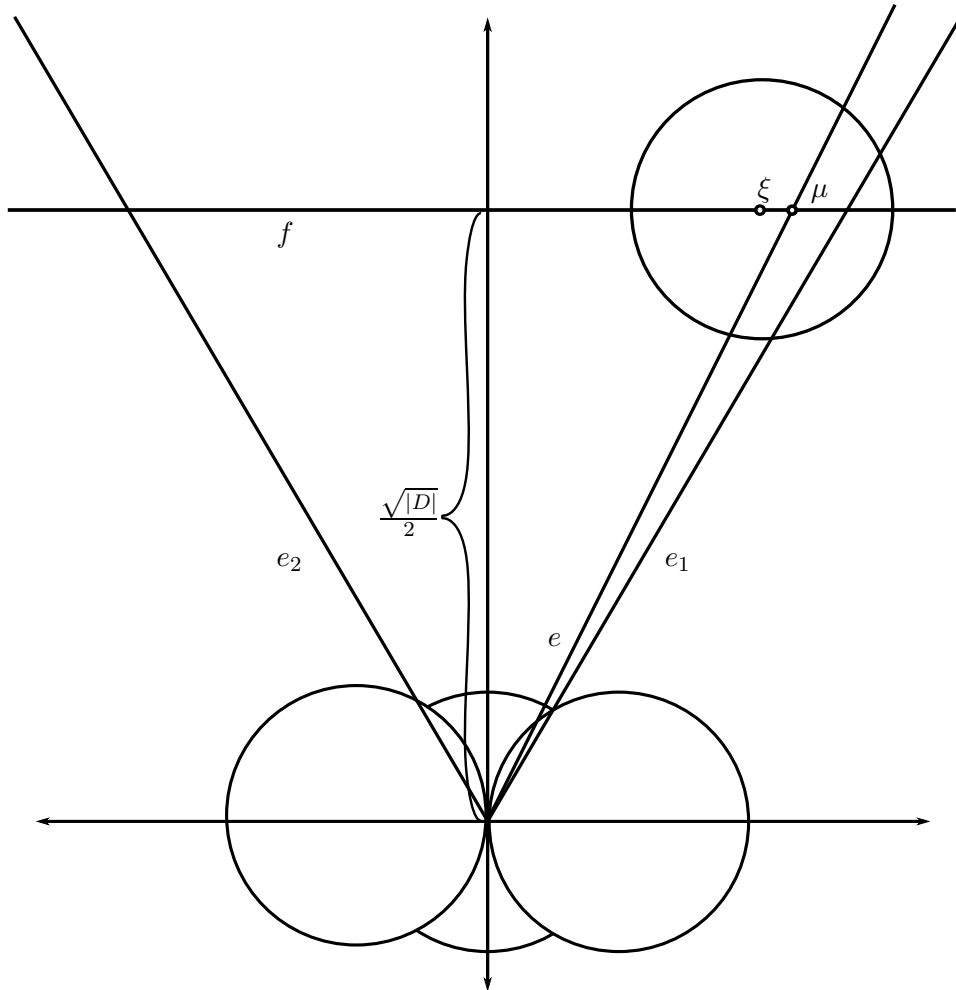


Figure 3. (Reproduced, with minor modifications, from [Zau83].)

It follows that the unit disc centered at ξ intersects e in a segment of total length > 1 . (Indeed, let τ be the point on e for which the line from ξ to τ is perpendicular to e , so that the distance from ξ to τ is strictly smaller than $\sqrt{3}/2$. Then by the Pythagorean theorem, τ divides the segment in question into two parts, each of length $> 1/2$.) Since $|\pi_1/\rho_1| \leq 1$, it follows that we can choose a rational integer γ so that $\gamma\pi_1/\rho_1$ lies within the open unit disc centered at ξ .

We claim that with the above choices of ξ and γ , both (P1) and (P2) hold. Condition (P2) is guaranteed by the choice of γ , so it remains only to verify (P1). For this it is enough to prove that ξ is prime. Indeed, suppose

that ξ is prime but (P1) fails. Then

$$\rho_1 \xi = \pi_1 \kappa$$

for some κ . Since ξ is prime, it must divide either π_1 or κ . But ξ cannot divide π_1 ; if it did, then since π_1 is irreducible, we would have that π_1 is a unit multiple of ξ . But then π_1 would be prime since ξ is prime. This contradicts the observation made above that none of the π_i are prime. So ξ must divide κ ; but then dividing through by ξ we find that π_1 divides ρ_1 . That implies that π_1 and ρ_1 are unit multiples of each other, which again contradicts our initial observations.

Why should ξ be prime? Since ξ is a point of the lattice $\mathbf{Z} + \mathbf{Z}\eta$ lying on f , we have $\xi = n + \eta$ for some integer n . Moreover, since ξ belongs to the 60° angle determined by e_1 and e_2 , we find that

$$|(n-1) + 1/2| = |n - 1/2| \leq \frac{1}{2} \sqrt{|D|/3}.$$

But now (ii) of Theorem 1.10 implies that

$$\begin{aligned} \mathcal{N}(\xi) &= n^2 - n + A \\ &= (n-1)^2 + (n-1) + A \end{aligned}$$

is prime, so that ξ is a prime element of $\mathbf{Z}[\eta]$ by Lemma 1.13. \square

A small amount of computation shows that condition (ii) of Theorem 1.10 holds for the values $A = 2, 3, 5, 11, 17$, and 41 . This yields the following corollary:

Corollary 1.14. $\mathbf{Z}[(-1 + \sqrt{D})/2]$ is a unique factorization domain for $D = -7, -11, -19, -43, -67, -163$.

Checking larger values of A does not appear to yield any more examples satisfying the conditions of Theorem 1.10. Whether or not the list in Corollary 1.14 is complete is known as the *class number 1 problem*; an equivalent question appears in Gauss's *Disquisitiones* (see [Gau86, Art. 303]). In 1933, Lehmer showed [Leh33] that any missing value of A is necessarily large, in that $|D| > 5 \cdot 10^9$. In 1934, Heilbronn & Linfoot [HL34] showed that there is at most one missing value of A . Finally, in 1952, Heegner settled the problem, using new techniques from the theory of modular functions:

Theorem 1.15 (Heegner). *If $A > 41$, then $\mathbf{Z}[\eta]$ does not have unique factorization. Hence if $A \geq 2$ is an integer for which $n^2 + n + A$ is prime for all $0 \leq n < A - 1$, then $A \leq 41$.*

For a modern account of Heegner's proof, see [Cox89, §12].

9. Primes represented by general polynomials

The result of the previous section leaves a very natural question unresolved: Does Euler's polynomial $T^2 + T + 41$, which does such a marvelous job of producing primes at the first several natural numbers n , represent infinitely many primes as n ranges over the set of all positive integers? More generally, what can one say about the set of prime values assumed by a polynomial $F(T) \in \mathbf{Z}[T]$? In this section we survey the known results in this direction.

9.1. The linear case. Suppose first that $F(T)$ is linear, say $F(T) = a + mT$, where $m > 0$. Asking whether $F(n)$ is prime for infinitely many natural numbers n amounts to asking whether the infinite arithmetic progression

$$a + m, \quad a + 2m, \quad a + 3m, \quad a + 4m, \quad \dots$$

contains infinitely many primes — or, phrased in terms of congruences, whether or not there are infinitely many primes $p \equiv a \pmod{m}$.

This question is sometimes easy to answer. Let $d = \gcd(a, m)$. If $d > 1$, then there are at most finitely many primes in the above progression, since every term is divisible by d , and so we have a negative answer to our query. So let us suppose that $d = 1$. Then certain special cases can easily be settled in the affirmative. For example, if $a = -1$ and $m = 4$, then we are asking for infinitely many primes $p \equiv -1 \pmod{4}$, and now we can mimic Euclid: If there are only finitely many such primes, say p_1, \dots, p_k , form the number $N := 4p_1 \cdots p_k - 1$. Since $N \equiv -1 \pmod{4}$, it must have at least one prime divisor $p \equiv -1 \pmod{4}$. But p cannot be any of p_1, \dots, p_k , and we have a contradiction. A similar argument works when $a = -1$ and $m = 3$.

The general case of our problem is much more difficult. It turns out that whenever $\gcd(a, m) = 1$, there *are* infinitely many primes $p \equiv a \pmod{m}$. This was proved by Dirichlet in 1837, by analytic methods. (One can view his argument as a far-reaching generalization of Euler's proof that the sum of the reciprocals of the primes diverges.) We will give a proof of Dirichlet's theorem in Chapter 4.

For now we content ourselves with some special cases of Dirichlet's theorem that follow from algebraic arguments. We noted above that an easy variant of Euclid's proof shows that there are infinitely many primes p for which the residue class of p avoids the trivial subgroup of the unit group $(\mathbf{Z}/4\mathbf{Z})^\times$, and similarly for $(\mathbf{Z}/3\mathbf{Z})^\times$. As observed by A. Granville (unpublished), we have the following general result:

Theorem 1.16. *If H is a proper subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$, then there are infinitely many primes p for which $p \pmod{m} \notin H$.*

Proof. Let \mathcal{P} be the set of primes p for which $p \bmod m \notin H$, and let \mathcal{P}' be the set of such primes not dividing m . Assuming \mathcal{P} is finite, let P be the product of the elements of \mathcal{P}' . Fix an integer a coprime to m with $a \bmod m \notin H$ (which is possible since H is a *proper* subgroup), and then choose a positive integer n satisfying the congruences $n \equiv 1 \pmod{P}$ and $n \equiv a \pmod{m}$. (Such a choice of n is possible by the Chinese remainder theorem.) Since n is coprime to mP , none of its prime divisors can come from \mathcal{P} , so that every prime p dividing n must be such that $p \bmod m \in H$. But since H is closed under multiplication, this implies that $n \bmod m \in H$. This contradicts the choice of a . \square

If $F(T)$ is a nonzero polynomial with integer coefficients, we say that the prime p is a *prime divisor* of F if p divides $F(n)$ for some integer n . The following useful lemma is due to Schur [Sch12]:

Lemma 1.17. *Let $F(T)$ be a nonconstant polynomial with integer coefficients. Then F has infinitely many prime divisors.*

Proof. If $F(0) = 0$, then every prime is a prime divisor of F . So we can assume that the constant term c_0 (say) of $F(T)$ is nonzero. Then $F(c_0T) = c_0G(T)$ for some nonconstant polynomial $G(T)$ with constant term 1. It is enough to show that G has infinitely many prime divisors. Suppose that p_1, \dots, p_k is a list of prime divisors of G . For m sufficiently large, we have $|G(mp_1 \cdots p_k)| > 1$, so that there must be some prime p dividing $G(mp_1 \cdots p_k)$. Then p is a prime divisor of G and p is not equal to any of the p_i , since $G(mp_1 \cdots p_k) \equiv 1 \pmod{p_i}$ for each $1 \leq i \leq k$. So no finite list of prime divisors of G can be complete. \square

For example, let $F(T) = T^2 + 1$. If p divides $n^2 + 1$, then $n^2 \equiv -1 \pmod{p}$, and so either $p = 2$ or $p \equiv 1 \pmod{4}$. So Lemma 1.17 implies that there are infinitely many primes $p \equiv 1 \pmod{4}$. Similarly, if $F(T) = T^2 + T + 1$, then any prime divisor p of F is such that $p \equiv 1 \pmod{3}$, and so there are infinitely many primes $p \equiv 1 \pmod{3}$. Combining this with our earlier results, we have proved Dirichlet's theorem for all progressions modulo 3 and modulo 4.

These examples are special cases of the following construction: Recall that the m th *cyclotomic polynomial* is defined by

$$\Phi_m(T) = \prod_{\substack{1 \leq k \leq m \\ \gcd(k, m) = 1}} (T - e^{2\pi i k / m}),$$

i.e., $\Phi_m(T)$ is the monic polynomial in $\mathbf{C}[T]$ whose roots are precisely the primitive m th roots of unity, each occurring with multiplicity 1. For example, $\Phi_4(T) = T^2 + 1$ and $\Phi_3(T) = T^2 + T + 1$.

We will apply Lemma 1.17 to Φ_m to deduce that there are infinitely many primes $p \equiv 1 \pmod{m}$. To apply Lemma 1.17, we need that the coefficients of $\Phi_m(T)$ are not merely complex numbers, but in fact integers.

Lemma 1.18. *For each positive integer m , the polynomial $\Phi_m(T)$ has integer coefficients.*

Proof. For each m we have the factorization

$$(1.11) \quad T^m - 1 = \prod_{d|m} \Phi_d(T).$$

To see this, note that $T^m - 1 = \prod_{\zeta^{m=1}} (T - \zeta)$. Since the set of m th roots of unity is the disjoint union of the primitive d th roots of unity, taken over those d dividing m , we have (1.11). Applying Möbius inversion to (1.11) yields

$$\Phi_m(T) = \prod_{d|m} (T^d - 1)^{\mu(m/d)} = \frac{\prod_{d|m, \mu(m/d)=1} (T^d - 1)}{\prod_{d|m, \mu(m/d)=-1} (T^d - 1)} = \frac{F}{G},$$

say. Now F and G are *monic* polynomials in $\mathbf{Z}[T]$ with $G \neq 0$, and so we can write

$$(1.12) \quad F = GQ + R,$$

where $Q, R \in \mathbf{Z}[T]$ and $\deg R < \deg G$. Of course (1.12) remains valid over $\mathbf{C}[T]$ and expresses in that ring one result of division by G . But we know that over $\mathbf{C}[T]$, we have $F = G\Phi_m$, so that G goes into F with no remainder. By the uniqueness of quotient and remainder in the division algorithm for polynomials, we must have $R = 0$ above. Consequently, $\Phi_m = F/G = Q \in \mathbf{Z}[T]$. \square

Lemma 1.19. *If p is a prime divisor of Φ_m , then either $p \mid m$ or $p \equiv 1 \pmod{m}$.*

Proof. If p is a prime divisor of Φ_m , then p divides $\Phi_m(n)$ for some integer n . Since the cyclotomic polynomials have integer coefficients, it follows from (1.11) that $p \mid \prod_{d|m} \Phi_d(n) = n^m - 1$, so that the order of n modulo p is a divisor of m .

Suppose now that p does not divide m . We claim that in this case, m is the precise order of n modulo p . Thus m divides $p-1$, whence $p \equiv 1 \pmod{m}$. To prove the claim, suppose for the sake of contradiction that $f < m$ is the exact order of $n \pmod{p}$. Then f is a proper divisor of m . Moreover, p divides $n^f - 1 = \prod_{e|f} \Phi_e(n)$, so that p divides $\Phi_e(n)$ for some $e \mid f$. Hence the residue class $n \pmod{p}$ is a zero of both $\Phi_e(T)$ and $\Phi_m(T)$. The polynomials Φ_e and Φ_m both appear in the factorization (1.11) of $T^m - 1$, so that $T^m - 1$ has a

zero of order ≥ 2 over $\mathbf{Z}/p\mathbf{Z}$. But $T^m - 1$ has no multiple roots over $\mathbf{Z}/p\mathbf{Z}$, since $T^m - 1$ has no roots in common with its derivative mT^{m-1} . \square

Since only finitely many primes divide m , Lemmas 1.17 and 1.19 have the following corollary:

Corollary 1.20. *For each natural number m , there are infinitely many primes $p \equiv 1 \pmod{m}$.*

This proof of Corollary 1.20 is essentially due to Wendt [Wen95].

How far can one take this algebraic approach? The following result is due to Schur (op. cit.).

★ Theorem 1.21. *Let m be a positive integer and let H be a subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$. There is a nonconstant polynomial $F(T) \in \mathbf{Z}[T]$ with the following property: Every prime divisor p of F , with finitely many exceptions, satisfies $p \bmod m \in H$. Consequently, there are infinitely many primes p for which $p \bmod m \in H$.*

When H is the trivial subgroup we have just seen that $F := \Phi_m$ satisfies the conclusion of Theorem 1.21.

Schur gave an elementary proof of Theorem 1.21 requiring only familiarity with the theory of finite fields. A less elementary proof is outlined in Exercise 19. When m is a prime number, Theorem 1.21 is contained in the results of Chapter 2 (see, in particular, Theorem 2.15).

Suppose that a and m satisfy $a^2 \equiv 1 \pmod{m}$, where $a \not\equiv 1 \pmod{m}$. Applying Theorem 1.21 to the 2-element subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by $a \bmod m$, we obtain a polynomial $F(T)$ all of whose prime divisors (with finitely many exceptions) satisfy either $p \equiv 1 \pmod{m}$ or $p \equiv a \pmod{m}$. Schur showed (op. cit.) that if there is a single, suitably large prime $p \equiv a \pmod{m}$, then the polynomial F he constructs cannot have all (or even all but finitely many) of its prime divisors from the progression $1 \bmod m$. (See the first example below for an illustration of how this works.) So F must have infinitely many prime divisors $p \equiv a \pmod{m}$.

Since Dirichlet's theorem is true, there is always a suitably large prime $p \equiv a \pmod{m}$ to be used in Schur's argument, and so in principle, it is possible to give a purely algebraic proof of Dirichlet's theorem for any progression $a \bmod m$ satisfying $a^2 \equiv 1 \pmod{m}$. Moreover, this is best possible in the following sense:

★ Theorem 1.22 (Murty [Mur88, MT06]). *Suppose m is a positive integer. If F is a nonconstant polynomial with the property that every prime divisor p of F , with finitely many exceptions, satisfies $p \equiv 1 \pmod{m}$ or $p \equiv a \pmod{m}$, then $a^2 \equiv 1 \pmod{m}$.*

The proof of Theorem 1.22 rests on rather deep results in algebraic number theory. The principal tool required is the *Chebotarev density theorem*, which is a far-reaching generalization of Dirichlet's theorem. See [SL96] for a down-to-earth discussion of Chebotarev's result.

Example. As an easy example of Schur's method, consider the problem of showing that there are infinitely many primes $p \equiv 3 \pmod{8}$. We start by taking $F(T) := T^2 + 2$. From the elementary theory of quadratic residues we have that each odd prime divisor of $F(T)$ satisfies $p \equiv 1$ or $3 \pmod{8}$. Now we observe that there is at least one prime in the residue class $3 \pmod{8}$, namely 11. We replace T by $4T + 3$ and so obtain from F the polynomial

$$G(T) = F(4T + 3) = 16T^2 + 24T + 11 = 8(2T^2 + 3T) + 11.$$

Then every prime divisor of G belongs to either the residue class $1 \pmod{8}$ or $3 \pmod{8}$. Moreover, for each positive integer n , there is at least one prime $p \equiv 3 \pmod{8}$ for which $p \mid G(n)$, since $G(n) \equiv 3 \pmod{8}$. We will show that G (and hence also F) must have infinitely many prime divisors from the residue class $3 \pmod{8}$. Suppose otherwise, and let p_1, p_2, \dots, p_k be a complete list of the prime divisors $p \equiv 3 \pmod{8}$ of G . For each p_i , choose an integer n_i for which $G(n_i) \not\equiv 0 \pmod{p_i}$. (This is possible since G has at most two roots modulo p_i .) If n is a positive integer chosen by the Chinese remainder theorem to satisfy $n \equiv n_i \pmod{p_i}$ for all $1 \leq i \leq k$, then $G(n)$ cannot be divisible by any of p_1, \dots, p_k . So $G(n)$ must have a prime divisor from the residue class $3 \pmod{8}$ other than p_1, \dots, p_k – a contradiction.

Example. Since every integer a coprime to 24 satisfies $a^2 \equiv 1 \pmod{24}$, it is in principle possible to give an algebraic proof of Dirichlet's theorem for progressions with common difference 24. The details in this case have been completely worked out by Bateman & Low [BL65]. We leave to the reader the task of showing that 24 is the largest modulus m with the property that $a^2 \equiv 1 \pmod{m}$ for each a coprime to m .

9.2. Hypothesis H.

I do not mean to deny that there are mathematical truths, morally certain, which defy and will probably to the end of time continue to defy proof, as, *e.g.*, that every indecomposable polynomial function must represent an infinitude of primes. – J. J. Sylvester [Syl188]

There are two natural directions we might head in if we hope to generalize Dirichlet's result: First, we might inquire about simultaneous prime values of several linear polynomials. One has to be careful here, of course. For example, we cannot hope that there are infinitely many n for which both n and $n + 1$ are prime, because one of these two numbers is always

even! However if instead of n and $n + 1$ we consider n and $n + 2$, then this obstruction disappears, and we arrive at the following famous conjecture:

Conjecture 1.23 (Twin prime conjecture). *There are infinitely many natural numbers n for which both n and $n + 2$ are prime.*

Alternatively, we might accept the restriction of working with a single polynomial, but hope to treat polynomials of higher degree. The following conjecture of Euler, which appears in correspondence with Goldbach, fits nicely into this framework:

Conjecture 1.24 (Euler). *There are infinitely many natural numbers n for which $n^2 + 1$ is prime.*

Similarly, it seems reasonable to conjecture that our old friend, $T^2 + T + 41$, represents infinitely many primes. Once again, formulating conjectures of this type requires some care; if $n^2 + 1$ or $n^2 + n + 41$ is replaced by $n^2 + n + 2$, then the statement corresponding to Euler's conjecture is false, since $n^2 + n + 2$ is always even.

Suppose more generally that $F_1(T), \dots, F_r(T) \in \mathbf{Z}[T]$ are nonconstant polynomials, each with positive leading coefficient. We can ask when it is the case that $F_1(n), \dots, F_r(n)$ are simultaneously prime for infinitely many natural numbers n . Evidently if this is to be the case, then we must suppose that each F_i is irreducible over \mathbf{Z} . The example of $r = 2$ and $F_1(T) = T$, $F_2(T) = T + 1$ shows that this is not sufficient, as does the example of $r = 1$ and $F_1(T) = T^2 + T + 2$. What goes wrong in these examples is that there is a *local obstruction*: if we put $G(T) := \prod_{i=1}^r F_i(T)$, then $G(n)$ is always even. In 1958, Schinzel conjectured (see [SS58]) that these are the only remaining obstructions to be accounted for:

Conjecture 1.25 (Schinzel's 'Hypothesis H'). *Suppose $F_1(T), \dots, F_r(T) \in \mathbf{Z}[T]$ are nonconstant and irreducible and that each F_i has a positive leading coefficient. Put $G(T) := \prod_{i=1}^r F_i(T)$, and suppose that there is no prime p which divides $G(n)$ for every integer n . Then $F_1(n), F_2(n), \dots, F_r(n)$ are simultaneously prime for infinitely many natural numbers n .*

The hypothesis on G is necessary: Suppose that p is a (fixed) prime which divides $G(n)$ for each n . Then p divides some $F_i(n)$ for each n . But for large n , each $F_i(n) > p$, and so for large n , some $F_i(n)$ is composite.

The twin prime conjecture corresponds to choosing $r = 2$, $F_1(T) = T$, and $F_2(T) = T + 2$ in Hypothesis H. Taking instead $r = 1$ and $F_1(T) = T^2 + 1$, we recover Euler's Conjecture 1.24. Despite substantial attention, both the twin prime conjecture and Conjecture 1.24 remain open. Even more depressing, no case of Hypothesis H has ever been shown to hold except

when $r = 1$ and $F_1(T)$ is linear, when Hypothesis H reduces to Dirichlet's theorem!

Sieve methods, which we introduce in Chapter 6, can be used to obtain certain approximations to Hypothesis H. We give two examples: A theorem of Chen [Che73] asserts that there are infinitely many primes p for which $p + 2$ is either prime or the product of two primes. And Iwaniec [Iwa78] has shown that there are infinitely many n for which $n^2 + 1$ is either prime or the product of two primes. (This latter result applies also to $n^2 + n + 41$, and in fact to any quadratic obeying the conditions of Hypothesis H.)

10. Primes and composites in other sequences

We conclude by discussing the occurrence of primes in other sequences of interest. Results in this area are rather thin on the ground, and so we content ourselves with a smattering of problems and results meant to showcase our collective ignorance.

One sequence that has received much attention is that of the *Mersenne numbers* $2^n - 1$. The occurrence of primes in this sequence has long been of interest in view of Euclid's result that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is a perfect number. (Here a number is called *perfect* if it is the sum of its proper divisors.) Since $2^d - 1$ divides $2^n - 1$ whenever d divides n , for $2^n - 1$ to be prime it is necessary that n be prime. At first glance it appears that $2^p - 1$ is often prime; 7 of the first 10 primes p have this property. However, the tide quickly turns: Of the 78498 primes p up to 10^6 , only 31 yield primes. As of February 2009, there are 46 known primes of the form $2^p - 1$, the largest corresponding to $p = 43112609$. It is not clear from this data whether or not we should expect infinitely many primes of this form, but probabilistic considerations to be discussed in Chapter 3 suggest that we should:

Conjecture 1.26. *For infinitely many primes p , the number $2^p - 1$ is prime.*

Unfortunately, this conjecture seems far beyond reach. In fact, we know disturbingly little about the numbers $2^p - 1$; perhaps the most striking illustration of this is that even the following modest conjecture remains unproved:

Conjecture 1.27. *For infinitely many primes p , the number $2^p - 1$ is composite.*

We may also change the ‘ $-$ ’ sign to a ‘ $+$ ’ and consider primes of the form $2^n + 1$. Since $2^d + 1$ divides $2^n + 1$ when n/d is odd, we see that $2^n + 1$ can be prime only if n is a power of 2. This leads us to consider the *Fermat numbers* $F_m = 2^{2^m} + 1$. The attentive reader will recall that these numbers

appeared already in Goldbach's proof of Theorem 1.1. For $m = 0, 1, 2, 3$, and 4, the numbers F_m are prime:

$$2^{2^0} + 1 = 3, \quad 2^{2^1} + 1 = 5, \quad 2^{2^2} + 1 = 17, \quad 2^{2^3} + 1 = 257, \quad 2^{2^4} + 1 = 65537.$$

Fermat was intuitively certain that F_m is prime for all $m \geq 0$, and expressed this belief in letters to his contemporaries. But in 1732 Euler discovered the factorization

$$2^{2^5} + 1 = 641 \cdot 6700417.$$

It is now known that F_m is composite for $5 \leq m \leq 32$, and (for the same probabilistic reasons alluded to above) it is widely believed that F_m is composite for every $m \geq 5$. So much for intuition! Despite this widespread belief, the following conjecture appears intractable:

Conjecture 1.28. *The Fermat number F_m is composite for infinitely many natural numbers m .*

Similarly, for each even natural number a , one can look for primes in the sequence $a^{2^m} + 1$. Again we believe that there should be at most finitely many, but again the analogue of Conjecture 1.28 seems impossibly difficult! Indeed, there is no specific even number a for which we can prove that $a^{2^m} + 1$ is composite infinitely often. This is a somewhat odd state of affairs in view of the following amusing theorem of Schinzel [**Sch63**]:

Theorem 1.29. *Suppose that infinitely many of the Fermat numbers F_j are prime. If $a > 1$ is an integer not of the form 2^{2^r} (where $r \geq 0$), then $a^{2^m} + 1$ is composite for infinitely many natural numbers m .*

Proof. Fix an integer $a > 1$ not of the form 2^{2^r} . Let M_0 be an arbitrary positive integer. We will show that $a^{2^m} + 1$ is composite for some $m \geq M_0$.

Let F_j be a prime Fermat number not dividing $a(a^{2^{M_0}} - 1)$. Since a is coprime to F_j , Fermat's little theorem implies that

$$a^{F_j-1} = a^{2^{2^j}} \equiv 1 \pmod{F_j}.$$

Since $F_j \nmid a^{2^{M_0}} - 1$, we must have $M_0 < 2^j$. So we can write

$$\begin{aligned} a^{F_j-1} - 1 &= a^{2^{2^j}} - 1 \\ &= (a^{2^{M_0}} - 1)(a^{2^{M_0}} + 1)(a^{2^{M_0+1}} + 1)(a^{2^{M_0+2}} + 1) \cdots (a^{2^{2^j-1}} + 1). \end{aligned}$$

Since F_j divides $a^{F_j-1} - 1$ but not $a^{2^{M_0}} - 1$, it must be that F_j divides $a^{2^m} + 1$ for some $M_0 \leq m < 2^j$. We cannot have $a^{2^m} + 1 = F_j$, since a is not of the form 2^{2^r} , and so $a^{2^m} + 1$ is composite. \square

In connection with Fermat-type numbers the following result of Shapiro & Sparer [SS72] merits attention (cf. [Sha83, Theorem 5.1.5]). It shows (in particular) that the doubly exponential sequences $a^{2^m} + 1$ are unusually difficult to handle among sequences of the same general shape:

★ **Theorem 1.30.** *Suppose a, b , and c are integers, and that $a, b > 1$. If c is odd, then*

$$a^{b^m} + c$$

is composite for infinitely many $m \in \mathbf{N}$, except possibly in the case when a is even, $c = 1$, and $b = 2^k$ for some $k \geq 1$. If c is even, there are infinitely many such m except possibly when a is odd and $c = 2$.

The reader should note that the Shapiro–Sparer paper contains several other attractive results on composite numbers in various sequences.

We close this section by considering the sequence of shifted factorials $n! + 1$. Here we can easily obtain infinitely many composite terms, since Wilson’s theorem implies that $(p - 1)! + 1$ is composite for each $p > 3$. The following pretty theorem of Schinzel [Sch62b] generalizes this result:

Theorem 1.31. *Let α be a positive rational number. Then there are infinitely many n for which $\alpha \cdot n! + 1$ is composite.*

Lemma 1.32. *Let p be a prime and let r and s be positive integers. Then for $0 \leq i \leq p - 1$, we have*

$$p \mid si! + (-1)^{i+1}r \iff p \mid r(p - 1 - i)! + s.$$

Proof. By Wilson’s theorem,

$$\begin{aligned} -1 &\equiv (p - 1)! = (p - 1)(p - 2) \cdots (p - i)(p - i - 1)! \\ &\equiv (-1)^i i! (p - 1 - i)! \pmod{p}, \end{aligned}$$

so that $(p - 1 - i)! i! \equiv (-1)^{i+1} \pmod{p}$. Since p and $(p - 1 - i)!$ are coprime,

$$\begin{aligned} p \mid si! + (-1)^{i+1}r &\iff p \mid s(p - 1 - i)! i! + (-1)^{i+1}r(p - 1 - i)! \\ &\iff p \mid (-1)^{i+1}s + (-1)^{i+1}r(p - 1 - i)! \\ &\iff p \mid s + r(p - 1 - i)!. \quad \square \end{aligned}$$

Proof of Theorem 1.31. Write $\alpha = r/s$, where r and s are relatively prime positive integers. Assume $l \in \mathbf{N}$ and $l \geq r/2$. Then $(4l)!\alpha^{-1}$ is an integer divisible by both 4 and r . Since $4 \mid (4l)!\alpha^{-1}$, we can choose a prime $p_l \equiv -1 \pmod{4}$ with

$$p_l \mid (4l)!\alpha^{-1} - 1.$$

Because $r \mid (4l)!\alpha^{-1}$, necessarily $p_l \nmid r$. Since

$$(1.13) \quad p_l \mid r \left((4l)!\alpha^{-1} - 1 \right) = s(4l)! - r,$$

we must have $p_l > 4l$. From Lemma 1.32 (with $i = 4l$) and (1.13), we find that

$$(1.14) \quad p_l \mid r(p_l - 4l - 1)! + s.$$

Since $p_l \nmid r$, (1.14) implies that $p_l \nmid s$, and so

$$p_l \mid N_l := \alpha(p_l - 4l - 1)! + 1$$

whenever N_l is an integer. This happens for all large l : Indeed, from (1.14) we have $N_l \geq p_l/s \geq 4l/s$, so that $N_l \rightarrow \infty$ with l , which is only possible if $p_l - 4l - 1 \rightarrow \infty$ with l . But N_l is an integer whenever $p_l - 4l - 1 \geq s$.

Finally, notice that for large l , we cannot have $p_l = N_l$, since $p_l \equiv -1 \pmod{4}$ while $N_l \equiv 1 \pmod{4}$. Thus N_l is a composite integer of the form $\alpha \cdot n! + 1$. Letting $l \rightarrow \infty$, we obtain infinitely many composite numbers of this form. \square

Notes

Most of the proofs discussed for the infinitude of the primes may be found in [Dic66, Chapter XVIII] or [Nar00, §1.1]. For other compilations, see [Rib96, Chapter 1], [FR07, Chapter 3], and [Moh79]. Other elementary proofs of the stronger result that $\sum 1/p$ diverges may be found in [Bel43], [Mos58], and the survey [VE80].

The following result of Matijasevich and Putnam provides an interesting contrast to Goldbach's theorem (Theorem 1.9): *There is a polynomial with integral coefficients such that the set of primes coincides with the set of positive values assumed by this polynomial, as the variables range over the nonnegative integers.* (An explicit example of such a polynomial, in 26 variables, was produced by Jones et al. [JSWW76].) Yet upon inspection we realize we are once again looking at a result that properly belongs not to number theory but to computability theory (or logic); an analogous statement is true if we replace the set of primes with any *listable set*. Here a set of positive integers S is called *listable* if there is a computer program which, when left running forever, outputs precisely the elements of S . A very approachable introduction to this circle of ideas is Matijasevich's article [Mat99]; for complete details see [Mat93].

In connection with the results of §8, we cannot resist pointing out the remarkable identity

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999925\dots,$$

which shows that $e^{\pi\sqrt{163}}$ is very nearly an integer. We sketch the explanation, which comes from the theory of modular functions; for details one may consult [Cox89, §11]. Every lattice $L \subset \mathbf{C}$ has a so-called j -invariant $j(L)$,

and $j(L_1) = j(L_2)$ precisely when L_1 and L_2 are homothetic, i.e., when one can be obtained from the other by rotation and scaling. We view j as a function on the upper-half plane $\{z \in \mathbf{C} : \Im(z) > 0\}$ by defining $j(\tau)$ as $j(L)$, where L is the lattice spanned by 1 and τ . It turns out that j is then holomorphic on the upper half-plane. Moreover, since 1 and τ determine the same lattice as 1 and $\tau + 1$, we have $j(\tau) = j(\tau + 1)$. This shows that $j(\tau)$ is holomorphic as a function of $q = e^{2\pi i\tau}$ in the punctured disc $0 < |q| < 1$, and so j has a Laurent expansion. It turns out that this expansion starts

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots,$$

so that $j(\tau) \approx 1/q + 744$ for small q . Now for the coup de grâce: One can show that if K is an imaginary quadratic field with integral basis $1, \tau$, then $j(\tau)$ is an algebraic integer of degree exactly $h(K)$, the class number of K . In particular, if K has class number 1, then $j(\tau)$ is a rational integer. The main theorem of §8 implies that $K = \mathbf{Q}(\sqrt{-163})$ has class number 1, and so $j(\tau) \in \mathbf{Z}$ for $\tau = \frac{1+i\sqrt{163}}{2}$. This value of τ corresponds to $q = -1/\exp(\pi\sqrt{163})$, so that

$$e^{\pi\sqrt{163}} \approx j(\tau) - 744 \in \mathbf{Z}.$$

We remark that $e^{\pi\sqrt{163}}$ is actually transcendental, as may be deduced from the following theorem of Gelfond and Schneider (noting that $e^{\pi\sqrt{163}} = (-1)^{i\sqrt{163}}$): *If α and β are algebraic numbers, where $\alpha \neq 0$ and β is irrational, then α^β is transcendental.* Here “ α^β ” stands for $\exp(\beta \log \alpha)$, and any nonzero value of $\log \alpha$ is permissible. For a proof of the Gelfond–Schneider result, see, e.g., [Hua82, §17.9].

There are many sequences not discussed in §10 where it would be of interest to decide if they contain infinitely many primes, or composites. For example, fix a rational number $\alpha > 1$, and consider the sequence of numbers $\lfloor \alpha^n \rfloor$. Whiteman has conjectured that this sequence always contains infinitely many primes. If we drop the rationality condition, then from a very general theorem of Harman [Har97] we have that each sequence $\lfloor \alpha^n \rfloor$ contains infinitely many primes as long as $\alpha > 1$ avoids a set of measure zero. (Of course since the rational numbers have measure zero, this has no direct consequence for Whiteman’s conjecture.) Very little is known about the sequences considered by Whiteman. For the particular numbers $\alpha = 3/2$ and $\alpha = 4/3$, Forman & Shapiro [FS67] present ingenious elementary arguments showing that the sequence $\lfloor \alpha^n \rfloor$ contains infinitely many composite numbers. Some extensions of their results have been obtained by Dubickas & Novikas [DN05]; e.g., these authors prove that if $\xi > 0$ and $\alpha \in \{2, 3, 4, 6, 3/2, 4/3, 5/4\}$, then the sequence $\lfloor \xi \alpha^n \rfloor$ contains infinitely many composites.