Chapter 5

The distribution of prime numbers

5.1. Proofs that there are infinitely many primes

Exercise 5.1.1 (Proof #2)**.** Suppose that there are only finitely many primes, the largest of which is $n > 2$. Show that this is impossible by considering the prime factors of $n! - 1$.

Exercise 5.1.2. Prove that there are infinitely many composite numbers.

Exercise 5.1.3. Prove (5.1.1).

Exercise 5.1.4. Suppose that $p_1 = 2 < p_2 = 3 < \cdots$ is the sequence of prime numbers. Use the fact that every Fermat number has a distinct prime divisor to prove that $p_n \leq 2^{2^n} + 1$. What can one deduce about the number of primes up to x?

Exercise 5.1.5. (a) Show that if m is not a power of 2, then $2^m + 1$ is composite by showing that $2^a + 1$ divides $2^{ab} + 1$ whenever b is odd.
(b) Deduce that if $2^m + 1$ is prime, then there exists an integer n such that $m = 2^n$; that is, if $2^m + 1$ is prime, then it is a Fermat number $F_n = 2^{2^n} + 1$. (This also follows from exercise 3.9.3(b).)

5.2. Distinguishing primes

Exercise 5.2.1. Use this method to find all of the primes up to 200.

5.3. Primes in certain arithmetic progressions

Exercise 5.3.1. (a) Prove that any integer $\equiv a \pmod m$ is divisible by (a, m).
(b) Deduce that if $(a, m) > 1$ and if there is a prime $\equiv a \pmod m$, then that prime is (a, m).
(c) Give examples of arithmetic progressions which contain exactly one prime and examples which contain none.
(d) Show that the arithmetic progression $2 \pmod 6$ contains infinitely many prime powers.

Exercise 5.3.2. Use exercise 3.1.4(a) to show that if $n \equiv -1 \pmod 3$, then there exists a prime factor p of n which is $\equiv -1 \pmod 3$.

Exercise 5.3.3. Prove that there are infinitely many primes $\equiv -1 \pmod 4$.

Exercise 5.3.4. Prove that there are infinitely many primes $\equiv 5 \pmod 6$.

Exercise 5.3.5.† Prove that at least two of the arithmetic progressions mod 8 contain infinitely many primes.

5.4. How many primes are there up to x?

Exercise 5.4.1.† Assume the prime number theorem.

(a) Show that there are infinitely many primes whose leading digit is a "1". How about leading digit "7"?

(b) Show that for all $\epsilon > 0$, if x is sufficiently large, then there are primes between x and $x + \epsilon x$.

(c) Deduce that $\mathbb{R}_{\geq 0}$ is the set of limit points of the set $\{p/q : \ p, q \text{ primes}\}$.

(d) Let $a_1, \ldots, a_d$ be any sequence of digits, that is, integers between 0 and 9, with $a_1 \neq 0$. Show that there are infinitely many primes whose first (leading) d digits are $a_1, \ldots, a_d$.

Exercise 5.4.2.† Let $p_1 = 2 < p_2 = 3 < \cdots$ be the sequence of primes. Assume the prime number theorem and prove that

$$p_n \sim n \ \log n \quad \text{as } n \to \infty.$$

Exercise 5.4.3.† (a) Show that the sum of primes and prime powers $\leq x$ is $\sim x^2/(2\log x)$.

(b) Deduce that if the sum equals N, then $x \sim \sqrt{N \log N}$.

Exercise 5.4.4.‡ Use the prime number theorem in arithmetic progressions to prove that for any integers $a_1, \ldots, a_d, b_0, \ldots, b_d \in \{0, \ldots, 9\}$, with $a_1 \neq 0$ and $b_0 = 1$, 3, 7, or 9, there are infinitely many primes whose first d digits are $a_1, \ldots, a_d$ and whose last d digits are $b_d, \ldots, b_0$.

5.5. *Bounds on the number of primes*

Exercise 5.5.1.† Do better than this using Euler's result.

(a) Prove that $\sum_{n\geq 1} \frac{1}{n(\log n)^2}$ converges.

(b) Deduce that there are arbitrarily large x for which $\pi(x) > x/(\log x)^2$.

Exercise 5.5.2. Fix $\epsilon > 0$ arbitrarily small. Deduce Chebyshev's bounds (5.5.1) with $c_1 = \log 2 - \epsilon$ and $c_2 = \log 4 + \epsilon$, for all sufficiently large x, from Theorem 5.3.

Exercise 5.5.3. Use exercise 3.10.3 and the last displayed equation to prove that

$$\text{lcm}[m : \ m \leq n] \geq \frac{2^n}{n}. \tag{5.5.1}$$

5.6. *Gaps between primes*

Exercise 5.6.1. (a) Prove that there are gaps between primes $\leq x$ that are at least as large as the average gap between primes up to x.

(b) Prove that there are gaps between primes $\leq x$ that are no bigger than the average gap between primes up to x.

Exercise 5.6.2. (a) Show that if every interval $(x, x + 2\sqrt{x})$ contains a prime, then there are always primes between consecutive squares.

(b) Show that if there are always primes between consecutive squares, then every interval $(x, x + 4\sqrt{x} + 3]$ contains a prime.

Exercise 5.6.3. Deduce from this that there is a prime between any consecutive, sufficiently large, cubes.

Exercise 5.6.4. Prove that 2 and 3 are the only two primes that differ by 1.

5.7. *Formulas for primes*

Exercise 5.7.1. Show that if $f(x, y) \in \mathbb{Z}[x, y]$ has degree $d \geq 1$, then there are infinitely many pairs of integers m, n for which $|f(m, n)|$ is composite.

Exercise 5.7.2. Prove an analogous result for primes written in an arbitrary base $b \geq 3$.

Exercise 5.7.3.† Suppose that $f(x) = a_0 x + \cdots + a_d x^d \in \mathbb{Z}[x]$ with each $|a_i| \leq A$ and $a_d \neq 0$. Prove that if $f(n)$ is prime for some integer $n \geq A + 2$, then $f(x)$ is irreducible.

Additional exercises

Exercise 5.8.1. Let m be the product of the primes ≤ 1000. Prove that if n is an integer between 10^3 and 10^6, then n is prime if and only if $(n, m) = 1$.

Exercise 5.8.2. Show that if $p > 3$ and $q = p + 2$ are twin primes, then $p + q$ is divisible by 12.

Exercise 5.8.3. Show that there are infinitely many integers n for which each of $n, n+1, \ldots, n+1000$ is composite.

Exercise 5.8.4. Fix integer $m > 1$. Show that there are infinitely many integers n for which $\tau(n) = m$.

Exercise 5.8.5.† Fix integer $k > 1$. Prove that there are infinitely many integers n for which $\mu(n) = \mu(n + 1) = \cdots = \mu(n + k)$.

Exercise 5.8.6. Let H be a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$.

(a) Show that if a is coprime to m and q is a given non-zero integer, then there are infinitely many integers $n \equiv a \pmod m$ such that $(n, q) = 1$.
(b) Prove that if n is an integer coprime to m but which is not in a residue class of H, then n has a prime factor which is not in a residue class of H.
(c) Deduce there are infinitely many primes which do not belong to any residue class of H.

Exercise 5.8.7.† Suppose that for any coprime integers a and q there exists *at least one* prime $\equiv a \pmod q$. Deduce that for any coprime integers A and Q, there are *infinitely many* primes $\equiv A \pmod Q$.

Exercise 5.8.8. Prove that there are infinitely many primes p for which there exists an integer a such that $a^3 - a + 1 \equiv 0 \pmod p$.

Exercise 5.8.9. Prove that for any $f(x) \in \mathbb{Z}[x]$ of degree ≥ 1, there are infinitely many primes p for which there exists an integer a such that p divides $f(a)$.

Exercise 5.8.10. Let $\mathcal{L}(n) = \text{lcm}[1, 2, \ldots, n]$.

(a) Show that $\mathcal{L}(n)$ divides $\mathcal{L}(n + 1)$ for all $n \geq 1$.
(b) Express $\mathcal{L}(n)$ as a function of the prime powers $\leq n$.
(c) Prove that for any integer k there exist integers n for which $\mathcal{L}(n) = \mathcal{L}(n+1) = \cdots = \mathcal{L}(n+k)$.
(d)‡ Prove that if k is sufficiently large, then there is such an integer n which is $< 3^k$.

Exercise 5.8.11.† Prove that

$$\mathrm{Li}(x) \Big/ \frac{x}{\log x} \to 1 \quad \text{as} \quad x \to \infty.$$

Exercise 5.8.12. Prove that 1 is the best choice for B when approximating $\mathrm{Li}(x)$ by $x/(\log x - B)$.

Exercise 5.8.13.† Using the Maynard-Tao result, prove that there exists a positive integer $k \leq 246$ for which there are infinitely many prime pairs $p, p + k$.

Exercise 5.8.14. Suppose that a and b are integers for which $g(a) = 1$ and $g(b) = -1$, where $g(x) \in \mathbb{Z}[x]$.

(a) Prove that $b = a-2$, $a-1$, $a+1$, or $a+2$.

(b)† Deduce that there are no more than four integer roots of $(g(x)-1)(g(x)+1) = 0$.

(c)† Show that if $g(x)$ has degree 2 and there are four integer roots of $(g(x)-1)(g(x)+1) = 0$, then $g(x) = \pm h(x-A)$ where $h(t) = t^2 - 3t + 1$, with roots A, $A+1$, $A+2$, and $A+3$.

(d)† Modify the proof of Theorem 5.4 to establish that if $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 6$ and $|f(n)|$ is prime for $\geq d+3$ integers n, then $f(x)$ is irreducible.

Let $f(x) = h(x)h(x-4)$, which has degree 4. Note that $|f(n)|$ is prime for the eight values $n = 0, 1, \ldots, 7$, and so there is little room in which to improve (d).

Exercise 5.8.15.† Assume that there are infinitely many positive integers n for which $n^2 - 3n + 1$ is prime, and denote these integers by $n_1 < n_2 < \cdots$. Let $g_m(x) := (n_1 - x) \cdots (n_m - x)$. If ℓ is a positive integer for which $1 + \ell g_m(0), 1 + \ell g_m(1), 1 + \ell g_m(2), 1 + \ell g_m(3)$ are simultaneously prime, then prove that the polynomial $f(x) := (x^2 - 3x + 1)(1 + \ell g_m(x))$ has degree $d := m + 2$ and that there are exactly $d + 2$ integers n for which $|f(n)|$ is prime.

Appendix 5A. Bertrand's postulate and beyond

5.9. Bertrand's postulate

Exercise 5.9.1. Show that prime p does not divide $\binom{2n}{n}$ when $2n/3 < p \leq n$.

Exercise 5.9.2. Use Bertrand's postulate to prove that there are infinitely many primes with first digit "1".

Exercise 5.9.3. Use Bertrand's postulate to show, by induction, that every integer $n > 6$ can be written as the sum of distinct primes.

Exercise 5.9.4. Goldbach conjectured that every even integer ≥ 6 can be written as the sum of two primes. Deduce Bertrand's postulate from Goldbach's conjecture.

Exercise 5.9.5. Use Bertrand's postulate to prove that $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$ is never an integer.

Exercise 5.9.6. Prove that for every $n \geq 1$ one can partition the set of integers $\{1, 2, \ldots, 2n\}$ into pairs $\{a_1, b_1\}, \ldots, \{a_n, b_n\}$ such that each sum $a_j + b_j$ is a prime.

Exercise 5.9.7.† (a) Prove that prime p divides $\binom{2n}{n}$ when $n/2 < p \leq 2n/3$.

(b) Prove that the product of the primes in $(3m, 12m]$ divides $\binom{12m}{6m}\binom{6m}{4m}$.

(c)† Deduce that we can take any constant $c_2 > \frac{2}{9}\log(432)$ in (5.5.1).
(Note that $\frac{2}{9}\log(432) = 1.3485\ldots < \log 4 = 1.3862\ldots$.)

(d) Now deduce Bertrand's postulate for all sufficiently large x from (5.5.1).

5.10. The theorem of Sylvester and Schur

Exercise 5.10.1. Prove that $\left(1 + \frac{1}{x+k}\right)^k \leq \left(1 + \frac{k}{x+1}\right)$ for all $x \geq k \geq 1$.

Exercise 5.10.2. Prove that if $\pi(k) < \frac{k \log 4}{\log(2k)} - 1$ for all integers $k \geq 1$, then Theorem 5.7 holds for all $n \geq k \geq 1$.

Exercise 5.10.3. (a) Use Bertrand's postulate and the Sylvester-Schur Theorem to show that if $1 \leq r < s$, then there is a prime p that divides exactly one of the integers $r+1, \ldots, s$.

(b) Deduce that if $1 \leq r < s$, then $\frac{1}{r+1} + \cdots + \frac{1}{s}$ is never an integer.

Bonus read: A review of prime problems

5.11. Prime problems

Prime values of polynomials in one variable

Exercise 5.11.1. Give conditions on integers a, b, c, d with $a, c > 0$, assuming that $(a, b) = (c, d) = 1$, which guarantee that there are infinitely many integers n for which $an + b$ and $cn + d$ are different and both positive and odd. We conjecture, under these conditions that:

There are infinitely many pairs of primes $am + b, cm + d$.

Exercise 5.11.2.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many pairs of *consecutive* primes $p, p + 100$.

Exercise 5.11.3.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many triples of *consecutive* primes in an arithmetic progression.

Exercise 5.11.4.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many quadruples of *consecutive* primes formed of two pairs of prime twins.

Exercise 5.11.5.† Let $a_{n+1} = 2a_n + 1$ for all $n \geq 0$. Fix an arbitrarily large integer N. Use the prime k-tuplets conjecture to show that we can choose a_0 so that $a_0, a_1, \ldots, a_N$ are all primes.

Exercise 5.11.6. Show that the set of linear polynomials $a_1m + 1, a_2m + 1, \ldots, a_km + 1$, with each a_j positive, is admissible.

Exercise 5.11.7. Prove that the only prime pair $p, p^2 + 2$ is $3, 11$.

Exercise 5.11.8. (a) Prove that if $f_1 \cdots f_k$ has no fixed prime divisor, then, for each prime p, there are infinitely many integers n such that $f_1(n) \cdots f_k(n)$ is not divisible by p.

(b)† Show that if $p > \deg(f_1(x) \cdots f_k(x))$ and p does not divide $f_1(x) \cdots f_k(x)$, then n_p exists.

(c) Prove that if $f_j(x) = x + h_j$ for given integers $h_1, \ldots, h_k$, then n_p exists for a given prime p if and only if $\#\{\text{distinct } h_j \pmod p\} < p$.

Exercise 5.11.9.† (a)‡ Let $x_0, \ldots, x_m$ be variables. Prove that if $m > k \geq 0$, then

$$\sum_{S \subset \{1,2,\ldots,m\}} (-1)^{|S|} \Big(x_0 + \sum_{j \in S} x_j\Big)^k = 0.$$

(b) Deduce that if n has more than k different prime factors, then

$$\sum_{d|n} \mu(d)(\log(n/d))^k = 0.$$

(c)‡ What value does this take when n has exactly k different prime factors?

Exercise 5.11.10. Show that if each prime factor of n is $> n^{1/3}$, then n is either prime or the product of two primes.

Prime values of polynomials in several variables

Exercise 5.11.11. Let $g(x) = 1 + \prod_{j=1}^{k}(x - j)$. Prove that there exist integers a and b such that the reducible polynomial $f(x) = (ax + b)g(x)$ is prime when $x = n$ for $1 \leq n \leq k$. Compare this to the result in exercise 5.8.14(c) (with $d = k + 1$).

Goldbach's conjecture and variants

Exercise 5.11.12. Show that the Goldbach conjecture is equivalent to the statement that every integer > 1 is the sum of at most three primes

Appendix 5B. An important proof of infinitely many primes

5.12. Euler's proof of the infinitude of primes

Exercise 5.12.1. Show that if $\mathrm{Re}(s) > 1$, then

$$\left(1 - \frac{1}{2^{s-1}}\right) \sum_{n \geq 1} \frac{1}{n^s} = \sum_{\substack{n \geq 1 \\ n \text{ odd}}} \frac{1}{n^s} - \sum_{\substack{n \geq 1 \\ n \text{ even}}} \frac{1}{n^s}.$$

5.13. The sieve of Eratosthenes and estimates for the primes up to x

5.14. Riemann's plan for Gauss's prediction, I

Appendix 5C. What should be true about primes?

5.15. The Gauss-Cramér model for the primes

Appendix 5D. Working with Riemann's zeta-function

5.16. Riemann's plan for Gauss's prediction

Exercise 5.16.1. Prove that $\zeta(s) = 0$ has no zeros ρ with $\mathrm{Re}(\rho) > 1$.

5.17. Understanding the zeros

5.18. Reformulations of the Riemann Hypothesis

Exercise 5.18.1. (a) Prove that $\log(\mathrm{lcm}[1, 2, \ldots, N]) = \sum_{p^m \leq N} \log p$.
(b)† Use (4.11.1) to show that $\sum_{p^m \leq N} \log p = \sum_{ab \leq N} \mu(b) \log a$.
(c) Express $\mu(n)$ in terms of $\Omega(n)$ and $\omega(n)$.

Exercise 5.18.2. For any integer $m \geq 1$:
(a) Prove that there exists a constant c_m such that if $x \geq 2$, then

$$\int_2^x \frac{dt}{(\log t)^m} = \frac{x}{(\log x)^m} - c_m + m \int_2^x \frac{dt}{(\log t)^{m+1}}.$$

(b) Prove that there exists a constant C_m such that if $x \geq 2$, then

$$\mathrm{Li}(x) = \sum_{k=0}^{m-1} \frac{k!x}{(\log x)^{k+1}} - C_m + m! \int_2^x \frac{dt}{(\log t)^{m+1}}.$$

(c)† Prove that there exists a constant κ_m such that if $x \geq 3$, then

$$0 \leq \int_2^x \frac{dt}{(\log t)^{m+1}} \leq \frac{\kappa_m x}{(\log x)^{m+1}}.$$

Exercise 5.18.3. (a) Prove that $\overline{n^\rho} = n^{\overline{\rho}}$ for any integer n and $\rho \in \mathbb{C}$.

(b) Explain why if $\zeta(\rho) = 0$, then $\zeta(\overline{\rho}) = 0$.

(c) Show that if $\rho = \frac{1}{2} + i\gamma$, then

$$\frac{x^\rho}{\rho} + \frac{x^{\overline{\rho}}}{\overline{\rho}} = x^{1/2} \cdot \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{\frac{1}{4} + \gamma^2}.$$

(d) Show that if γ is large, then the expression in (c) is roughly $x^{1/2} \cdot \frac{2\sin(\gamma \log x)}{\gamma}$.

This exercise explains how (5.16.1) yields the approximation (5.17.1).

Appendix 5E. Prime patterns: Consequences of the Green-Tao Theorem

5.19. Generalized arithmetic progressions of primes

Consecutive prime values of a polynomial

Exercise 5.19.1. Show that if $i \neq j$ are integers and a and b are variables, then there do not exist integers u, v, w, not all zero, for which $u(b + ia + i^2) + v(b + ja + j^2) = w$.

Exercise 5.19.2. Prove that there exist infinitely many pairs of integers a and b such that the first k values of the polynomial $x^d + ax + b$ are all prime.

Magic squares of primes

Exercise 5.19.3. Prove that every 3-by-3 square of integers in arithmetic progressions along each row and column can be rearranged to form a 3-by-3 magic square and vice versa.

Primes as averages

Exercise 5.19.4. Prove that the averages of any two distinct elements of the set $2, 2^2, 2^3, \ldots, 2^m$ are distinct.

Exercise 5.19.5. Prove that the averages of any two distinct elements of A are distinct and prime.

Exercise 5.19.6.‡ Prove that there exist arbitrarily large sets A of primes such that the average of any subset of A yields a distinct prime (e.g $\{7, 19, 67\}$, $\{5, 17, 89, 1277\}$ and $\{209173, 322573, 536773, 1217893, 2484733\}$).

Appendix 5F. A panoply of prime proofs

Exercise 5.20.1. Show that $(q, mn) = 1$ and deduce that q has a prime factor not on our list.

Appendix 5G. Searching for primes and prime formulas

5.21. Searching for prime formulas

5.22. Conway's prime producing machine

5.23. Ulam's spiral

Exercise 5.23.1. Prove that we have

$$U(x,y) = \begin{cases} 4x^2 - x + 1 + y & \text{if } -x \le y \le x \text{ with } x \ge 0, \\ 4y^2 + y + 1 - x & \text{if } -y \le x \le y \text{ with } y \ge 0, \\ 4x^2 - 3x + 1 - y & \text{if } -|x| \le y \le |x| \text{ with } x \le 0, \\ 4y^2 + 3y + 1 + x & \text{if } -|y| < x \le |y| \text{ with } y \le 0. \end{cases}$$

Exercise 5.23.2. Let three consecutive values of a quadratic polynomial f be $f(n-1) = u, f(n) = v, f(n+1) = w$. Prove that f has discriminant $\left(\frac{u-4v+w}{2}\right)^2 - uw$.

5.24. Mills's formula

Appendix 5H. Dynamical systems and infinitely many primes

5.25. A simpler formulation

Exercise 5.25.1. Show that if $f_m(a) = a$, then $f_{m+n}(a) = f_n(a)$ for all $n \ge 0$.

5.26. Different starting points

Exercise 5.26.1. Perform a similar analysis of the map $x \to x^2 - 2$ beginning by studying the orbit of 0. (The orbit of 4 under this map is shown, in the Lucas-Lehmer test (Corollary 10.10.1), to provide an efficient way to test whether a given Mersenne number is prime.)

5.27. Dynamical systems and the infinitude of primes

5.28. Polynomial maps for which 0 is strictly preperiodic

Exercise 5.28.1. Suppose that $f(x)$ has an orbit $x_0 \to x_1 \to \cdots$. Let $g(x) = f(x+a) - a$. Prove that $g(x)$ has an orbit $x_0 - a \to x_1 - a \to x_2 - a \to \cdots$.

Exercise 5.28.2. Find every $f(x) \in \mathbb{Z}[x]$ with each of the four orbits above. (As an example, $f_0(x) = a$ gives $0 \to a \to a$, so $f(x)$ is another with this orbit if and only if 0 and a are roots of $f(x) - f_0(x)$; that is, $f(x) - f_0(x) = x(x-a)g(x)$ for some $g(x) \in \mathbb{Z}[x]$.)

Exercise 5.28.3.[‡] Prove that the four orbits above are the only possible ones.

Exercise 5.28.4. Let $f(x) \in \mathbb{Z}[x]$ and deduce from our classification of possible orbits:
(a) 0 is strictly preperiodic if and only if $f^2(0) = f^4(0) \ne 0$;
(b) $L(f) = \text{lcm}[f(0), f^2(0)] =: \ell(f)$ (as claimed in the proof of Theorem 5.9);
(c) x_0 has a wandering orbit if and only if $x_2 \ne x_4$.

Exercise 5.28.5. Suppose that $u_0 \in \mathbb{C}$ has period p under the map $x \to f(x)$ where $f(x) \in \mathbb{Z}[x]$, so that u is a root of the polynomial $f^p(x) - x$. Prove that if f is monic, then $\frac{u_j - u_i}{u_1 - u_0}$ is a unit for all $0 \le i < j \le p-1$.