Appendix A
Background

A.1 Sine, cosine, and exponentials

Theorem A.1. *For all complex numbers z,*

$$e^{iz} = \cos z + i \sin z.$$

Consequently,

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}$$

and

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}.$$

Proof. It is well known that for a complex number z

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!};$$

$$\cos z = \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k}}{(2k)!};$$

$$\sin z = \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k+1}}{(2k+1)!}.$$

Once we observe $i^{4k+1} = i$, $i^{4k+2} = -1$, $i^{4k+3} = -i$, $i^{4k} = 1$, the theorem is an easy consequence of these Taylor expansions. □

Theorem A.2. *There are n distinct complex numbers z such that $z^n = 1$. They can be expressed as*

$$e^{\frac{2\pi ik}{n}}, \quad k = 0, \ldots, n-1.$$

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

Proof. The equation $z^n = 1$ has at most n solutions. On the other hand, the above numbers, n distinct numbers, all satisfy the equation. □

The following property of the exponential function is the basis of Fourier theory:

Theorem A.3. *Let k be an integer. Then*

$$\int_0^1 e^{2\pi ikx}\,dx = \begin{cases} 1 & k = 0; \\ 0 & k \neq 0. \end{cases}$$

Proof. See Exercise A.1.1. □

A.2 The Binomial Theorem

For natural number n and k, with $0 \leq k \leq n$ we define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

The following theorem is fundamental:

Theorem A.4 (The Binomial Theorem). *If n is a natural number, then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof. The proof is an easy induction and ultimately relies on the fact that

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

□

We now use the Binomial Theorem to prove the following theorem:

Theorem A.5. *For $k, y \in \mathbb{N}$ define*

$$\sigma_k(y) = \sum_{m=1}^{y} m^k.$$

Then there is a polynomial $f_k(x)$ with rational coefficients with leading term $x^{k+1}/(k+1)$ such that

$$\sigma_k(y) = f_k(y).$$

Proof. We will prove the theorem by induction. For $k = 1$ we have

$$\sum_{m=1}^{y} m = \frac{1}{2}y^2 + \frac{1}{2}y.$$

Now suppose we know the theorem for every $l < k$. By the Binomial Theorem

$$(m + 1)^{k+1} - m^{k+1} = \sum_{j=0}^{k-1} \binom{k}{j} m^j.$$

As a result

$$(y + 1)^{k+1} - 1 = \sum_{m=1}^{y} \left\{(m + 1)^k - m^k\right\} = \sum_{j=0}^{k} \binom{k+1}{j} \sigma_j(y).$$

Consequently,

$$\binom{k+1}{k} \sigma_k(y) = (y + 1)^{k+1} - 1 - \sum_{j=0}^{k-1} \binom{k+1}{j} f_j(y).$$

By the induction hypothesis the right-hand side is a polynomial of degree $k + 1$ with leading term y^{k+1}. Once we observe

$$\binom{k+1}{k} = k + 1$$

the theorem follows. □

Corollary A.6. *For all natural numbers k,*

$$\sigma_k(y) = \frac{y^{k+1}}{k+1} + O(y^k).$$

A.3 The Pigeon-Hole Principle

The Pigeon-Hole Principle is the following intuitively obvious statement: If we distribute n balls among m boxes, with $n > m > 0$, then at least one box will end up with more than one ball. Stated differently, if we have n pigeon trying to get in m pigeon-holes, with $n > m > 0$, then at least one of the pigeon-holes will have two pigeons in it, hence the title *The Pigeon-Hole Principle*. The Pigeon-Hole Principle is also known as Dirichlet's Box Principle. Dirichlet (1834) used this principle to prove a theorem about rational approximation to irrational numbers. We present this theorem in Example A.11 below. The Pigeon-Hole Principle is an extremely useful statement with many applications. In this appendix we give a proof of this statement using mathematical induction. We then give several applications. The appendix ends with a few standard problems.

The Pigeon-Hole Principle should be thought of as a statement about functions. Let A be the set of pigeons and B the set of pigeon-holes. Then the process of sending pigeons to pigeon-holes is a function from $A \to B$. The technical statement of the Pigeon-Hole Principle is the following:

Theorem A.7. *Let A, B be finite sets with $\#A > \#B$. Then there are no injective maps $f : A \to B$.*

Proof. We will prove this by induction on $\#B$. If $\#B = 1$, and $\#A > 1$, it is clear that we cannot have an injective function $f : A \to B$ as there is only one option for the image of the function f. Now suppose $\#B = k \geq 2$ and that we know the theorem for every set of size $k - 1$. Suppose A is a set with $\#A > \#B$ and let $f : A \to B$ be an injective map. Pick an element $b \in B$. Since f is injective, $f^{-1}(b)$ consists of a single element $a \in A$. Then $\#(B - \{b\}) = k - 1$, and the restriction of f to $A - \{a\}$ gives a function $\tilde{f} : A - \{a\} \to B - \{b\}$. By the induction hypothesis this function $\tilde{f}$ is not injective, hence the original function f could not be injective. □

Similarly one can show that if we have sets A, B with $\#A > k\#B$ for some natural number k, then there is at least one element $b \in B$ such that

$$\#f^{-1}(b) \geq k + 1.$$

We now give some examples.

Example A.8. Of every eight people, there are at least two who are born on the same day of the week. Of every fifteen people, there are at least three born on the same day of the week.

Example A.9. Of every $n + 1$ integers, there are at least two with difference divisible by n. In order to see this write $\mathbb{Z}$ as the disjoint union of the following n subsets $\mathbb{Z}_a$, $0 \leq a \leq n - 1$. For each a, let $\mathbb{Z}_a$ be the set of integers k such that $k \equiv a \bmod n$. Since we have $n + 1$ elements and n sets $\mathbb{Z}_a$, there is an a with the property that $\mathbb{Z}_a$ contains at least two elements x, y of the set. Since $x \equiv a$ and $y \equiv a$, it follows $x \equiv y \bmod n$ and consequently, $n \mid x - y$.

Example A.10. We will show that of every five distinct real numbers at least two of them satisfy

$$0 < \frac{a - b}{1 + ab} < 1.$$

Let the five numbers be $a_1, \ldots, a_5$. Since the map $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ is a bijection, there will be five angles $\theta_i \in (-\pi/2, \pi/2)$, $1 \leq i \leq 5$, such that $a_i = \tan\theta_i$. Now divide up the interval $(-\pi/2, \pi/2)$ to four subintervals $(-\pi/2, -\pi/4]$, $(-\pi/4, 0]$, $(0, \pi/4]$, and $(\pi/4, \pi/2)$. Since we have five θ_i's and four subintervals, by the Pigeon-Hole Principle at least two of them will be in the same subinterval. This means that there are indices i, j such that

$$0 < \theta_i - \theta_j < \pi/4.$$

Since tan is monotone increasing on the interval $(-\pi/2, \pi/2)$, we have

$$\tan 0 < \tan(\theta_i - \theta_j) < \tan(\pi/4).$$

Now we recall $\tan 0 = 0$, $\tan(\pi/4) = 1$, and that for angles α, β,

$$\tan(\alpha - \beta) = \frac{\tan\alpha - \tan\beta}{1 + \tan\alpha \cdot \tan\beta}.$$

We finally get

$$0 < \frac{a_i - a_j}{1 + a_i a_j} < 1$$

and we are done.

Example A.11 (Dirichlet). If α is an irrational number, then there are infinitely many rational numbers p/q, with $\gcd(p, q) = 1$, such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Let n be a natural number. We will prove that there is a rational number p/q such that $1 \leq q \leq n$ with the property that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}. \tag{A.1}$$

It is not hard to see that the main claim of this example follows from this statement. Equation A.1 is equivalent to the existence of a pair of integers (p, q) with $1 \leq q \leq n$ such that

$$|q\alpha - p| < \frac{1}{n}.$$

Consider the fractional parts $\{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$. These are n numbers in the interval $(0, 1)$, and never a rational number, as otherwise α would be a rational number. In particular, each of them lands in the one of the following *pigeon-holes*: $(0, 1/n)$, $(1/n, 2/n), \ldots, (1 - 1/n, 1)$. If one of the $\{k\alpha\}$ falls in the first of these intervals $(0, 1/n)$, then we have $0 < \{k\alpha\} < 1/n$, which gives $0 < k\alpha - [k\alpha] < 1/n$. This verifies the assertion with $p = [k\alpha]$ and $q = k$. If none of the fractional parts falls in the first interval, then we have n fractional parts in $n - 1$ intervals. By the Pigeon-Hole Principle two of the fractional parts, $\{k\alpha\}$ and $\{l\alpha\}$ say, will be in the same interval. Without loss of generality assume $k > l$. Since the length of each of the intervals is $1/n$ we will have

$$|\{k\alpha\} - \{l\alpha\}| < 1/n.$$

The left-hand side of the inequality is equal to

$$|k\alpha - [k\alpha] - l\alpha + [l\alpha]| = |(k - l)\alpha - ([k\alpha] - [l\alpha])|.$$

The result follows with $q = (k - l) < n$ and $p = [k\alpha] - [l\alpha]$.

Exercises

A.1.1 Use Theorem A.1 or any other method to prove Theorem A.3.

A.1.2 Use Theorem A.1 to give a proof for the addition formula for sine and cosine:

$$\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta,$$

$$\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta.$$

A.1.3 Compute $\cos\frac{\pi}{7}\cdot\cos\frac{2\pi}{7}\cdot\cos\frac{3\pi}{7}$.

A.1.4 Compute the value of $\cos\frac{\pi}{7}-\cos\frac{2\pi}{7}+\cos\frac{3\pi}{7}$.

A.1.5 Let $\eta_1=1,\eta_2,\eta_3$ be the three third roots of 1 in $\mathbb{C}$. Find a formula for the value of $\eta_1^n+\eta_2^n+\eta_3^n$ for $n\in\mathbb{Z}$.

A.2.1 Show that for $n\in\mathbb{N}$,

$$\sum_{k=0}^{n}\binom{n}{k}=2^n,\quad \sum_{k=0}^{n}(-1)^k\binom{n}{k}=0.$$

A.2.2 Prove that for all natural numbers n,

$$\sum_{k=0}^{n}\binom{k}{r}=\binom{n+1}{r+1}.$$

A.2.3 Show that for all $n\in\mathbb{N}$,

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}.$$

A.2.4 Prove that for all natural n

$$\sum_{k=0}^{n}(-1)^k\binom{2n}{k}=\frac{-1}{n}\binom{2n}{n}.$$

A.2.5 Prove the identity

$$\sum_{k=1}^{n}k2^{-2k}\binom{2k}{k}=\frac{n(n+1)}{3\cdot 2^{2n+1}}\binom{2n+2}{n+1}.$$

A.2.6 Show that for all $n\in\mathbb{N}$, $n^2\mid(n+1)^n-1$.

A.2.7 Show that for all natural numbers n,k,

$$\frac{1}{k+1}n^{k+1}<\sum_{r=0}^{n}r^k<\left(1+\frac{1}{n}\right)^{k+1}\frac{1}{k+1}n^{k+1}.$$

A.3.1 Show that if we have six numbers from the set $\{1,2,\dots,10\}$ two of them add up to an odd number.

A.3.2 Show that if we have a subset $A \subset \{1, 2, \dots, 100\}$ with ten elements, then the set A has disjoint subsets S, T whose elements have the same sum.

A.3.3 Show that if we choose a subset $S \subset \{1, 2, \dots, 2n\}$ with $n + 1$ elements, then there are at least two integers $x, y \in S$ such that $x \mid y$.

A.3.4 Show that if we choose five points in a unit square, there are at least two of them that are at most $\sqrt{2}/2$ apart.

A.3.5 Show that of every group of n people there are two with an identical number of friends in the group.

A.3.6 Suppose we have an infinite array of natural numbers $(a_{ij})_{i,j \in \mathbb{N}}$ with the property that $a_{ij} \leq ij$. Show that for every natural number k, there is at least one natural number m which is repeated at least k times in the array.

Appendix B
Algebraic integers

Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. We write

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

with $a_n \neq 0$. Then n is called the degree, and a_n the *leading coefficient*. If the leading coefficient of f is equal to 1, then f is called *monic*. For example, $3x^5 - 7x + 1$ is a polynomial of degree 5 with leading coefficient 3, and the polynomial $x^7 - 10^{487}x^2 + 57$ is monic.

Definition B.1. A complex number α is called an *algebraic integer* if there is a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

For example, it is clear that all integers are algebraic integers, and numbers like $1/5$ and $327/82$ are not. The complex number i is an algebraic integer as it satisfies $f(i) = 0$ with $f(x) = x^2 + 1$. More generally, every element of $\mathbb{Z}[i]$ is an algebraic integer. Every root of unity is an algebraic integer. The quadratic irrationality $-\sqrt{2}$ is an algebraic integer since it satisfies the equation $x^2 - 2 = 0$.

Lemma B.2. *If α is an algebraic integer, then there is a monic polynomial $f \in \mathbb{Z}[x]$ such that f is irreducible over $\mathbb{Q}$, and*

$$f(\alpha) = 0.$$

Proof. This is immediate from Gauss's Lemma (Corollary to Theorem 3.1, [25, Ch. 3]). □

The irreducible polynomial f in Lemma B.2 is called the *minimal polynomial of α*.

The following corollary is immediate from the lemma.

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

Corollary B.3. *If a rational number γ is an algebraic integer, then $\gamma \in \mathbb{Z}$.*

The following theorem is the main result of this section:

Theorem B.4. *If α, β are algebraic integers, then so are $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$.*

The proof of the theorem requires a bit of preparation.

Definition B.5. A polynomial F in the n indeterminates $x_1, \dots, x_n$ is called *symmetric* if for every $\sigma \in S_n$, the group of permutations of the set $\{1, \dots, n\}$,

$$F(x_1, \dots, x_n) = F(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

For example, the polynomial $x + y$ is a symmetric polynomial of the two variables x, y. The polynomial $x + y^2$ is not symmetric. The polynomial

$$x^2 + y^2 + z^2$$

is symmetric in the three variables x, y, z.

The simplest symmetric polynomials in the n indeterminates $x_1, \dots, x_n$ are denoted by

$$s_1 = \sum_{1 \le i \le n} x_i;$$

$$s_2 = \sum_{1 \le i < j \le n} x_i x_j;$$

$$s_3 = \sum_{1 \le i < j < k \le n} x_i x_j x_k$$

$$\dots$$

$$s_n = x_1 \cdots x_n.$$

These symmetric polynomials occur in nature as the coefficients of the polynomials with roots $x_1, \dots, x_n$, i.e.,

$$(x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

Not only are the s_i's the simplest symmetric polynomials, they are in fact the building blocks of all symmetric polynomials in the variables $x_1, \dots, x_n$.

Theorem B.6. *Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be a symmetric polynomial. Then there is a polynomial $G \in \mathbb{Z}[x_1, \dots, x_n]$ such that*

$$F(x_1, \dots, x_n) = G(s_1, s_2, \dots, s_n).$$

Proof. Write F in the form

$$F(x_1, \dots, x_n) = \sum_{r_1, r_2, \dots, r_n \in \mathbb{N} \cup \{0\}} c(r_1, \dots, r_n) x_1^{r_1} \cdots x_n^{r_n}$$

with $c(r_1, \ldots, r_n) \in \mathbb{Z}$. Pick the n-tuple $(r_1, \ldots, r_n)$ with the following three properties:

- $c(r_1, \ldots, r_n) \neq 0$;
- $r_1 \geq \cdots \geq r_n$;
- $w = nr_1 + (n-1)r_2 + \cdots + r_n$ is maximal. Call w the weight of F and denote it by $w(F)$.

Now consider the polynomial

$$F_1(x_1, \ldots, x_n) := F(x_1, \ldots, x_n) - c(r_1, \ldots, r_n) s_1^{r_1-r_2} s_2^{r_2-r_3} \cdots s_{n-1}^{r_{n-1}-r_n} s_n^{r_n}.$$

It is easy to see that F_1 has integral coefficients and that $w(F_1) < w(F)$. Apply the same procedure to F_1 to obtain a polynomial F_2 with $w(F_2) < w(F_1)$. By repeating this process we obtain a sequence of symmetric polynomials $F, F_1, F_2, \ldots$ such that $w(F) > w(F_1) > w(F_2) > \ldots$. For some k, we will have $w(F_k) = 0$, and that means F_k is a constant. This proves the theorem. □

Now we can go back and prove our main theorem.

Proof of Theorem B.4. We will prove that $\alpha\beta$ is algebraic. The other cases are similar.

Suppose α satisfies the equation $f(\alpha) = 0$ with f a monic polynomial with integer coefficients. Write

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i).$$

The algebraic integer α is one of the α_i's. As $f \in \mathbb{Z}[x]$, we see that

$$s_1 = \sum_i \alpha_i,$$

$$s_2 = \sum_{i<j} \alpha_i \alpha_j,$$

$$\vdots$$

$$s_k = \alpha_1 \cdots \alpha_k,$$

are integers.

Similarly, β satisfies an algebraic equation $g(x) = 0$ with $g \in \mathbb{Z}[x]$ a monic polynomial. Write

$$g(x) = \prod_{i=1}^{l} (x - \beta_i).$$

The algebraic integer β is one of the β_i's. Then, as before, the complex numbers

$$t_1 = \sum_i \beta_i,$$

$$t_2 = \sum_{i<j} \beta_i \beta_j,$$

$$\vdots$$

$$t_l = \beta_1 \cdots \beta_l$$

are integers.

Now consider the equation

$$h(x) = \prod_{i=1}^{k} \prod_{j=1}^{l} (x - \alpha_i \beta_j).$$

This expression has $\alpha\beta$ as a root. Also, it is symmetric in the variables α_i's and in the variables β_j's, separately. We want to show $h(x) \in \mathbb{Z}[x]$.

First write

$$h(x) = \sum_{r_1,\ldots,r_k,t \in \mathbb{N}\cup\{0\}} c(r_1, \ldots, r_k, t)\alpha_1^{r_1} \ldots \alpha_k^{r_k} x^t$$

with $c(r_1, \ldots, r_k, t)$ symmetric polynomials with integer coefficients in β_j's. By Theorem B.6 and the earlier remarks $c(r_1, \ldots, r_k, t) \in \mathbb{Z}$. Now we write

$$h(x) = \sum_t c_t x^t$$

with

$$c_t = \sum_{r_1,\ldots,r_k} c(r_1, \ldots, r_k, t)\alpha_1^{r_1} \ldots \alpha_k^{r_k}.$$

Again another application of Theorem B.6 shows that each c_t is an integer and we are done. □

Remark B.7. There are several proofs for Theorem B.4. Here we briefly sketch two proofs of the theorem that rely on linear algebra methods. We encourage the reader to work out the details as an exercise.

The first proof uses the statement that a complex number α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is $\mathbb{Z}$-module of finite rank. Now let α, β be algebraic integers. Then it is easy to see that $\mathbb{Z}[\alpha, \beta]$ is a $\mathbb{Z}$-module of finite rank, which, by the classification theorem of $\mathbb{Z}$-modules of finite rank, is free. Next, since $\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, it follows that $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha + \beta]$ are $\mathbb{Z}$-submodules of $\mathbb{Z}[\alpha, \beta]$, and consequently free of finite rank. This statement implies that $\alpha\beta$ and $\alpha + \beta$ are algebraic integers.

Another beautiful argument which we learned from Antoine Chambert-Loir uses the notion of the *companion matrix* of a polynomial. Let α be an algebraic integer and f_α be its minimal polynomial, and let n_α be the degree of f_α. We let C_α be the companion matrix of f_α. By definition, the characteristic polynomial of C_α is the polynomial f_α. The Cayley–Hamilton Theorem implies that C_α satisfies $f_\alpha(C_\alpha) = 0$, but since f_α is irreducible, this implies that f_α is the minimal polynomial of C_α. Then $C_\alpha : \mathbb{C}^{n_\alpha} \to \mathbb{C}^{n_\alpha}$ is a linear transformation with the roots of f_α as its eigenvalues. Similarly, for an algebraic integer β, we define f_β, n_β, and $C_\beta : \mathbb{C}^{n_\beta} \to \mathbb{C}^{n_\beta}$ as above. Then the fact that $\alpha + \beta$ is an algebraic integer follows from the following two statements:

- $\alpha + \beta$ is an eigenvalue of $C_\alpha \otimes I_{n_\beta} + I_{n_\alpha} \otimes C_\beta : \mathbb{C}^{n_\alpha} \otimes \mathbb{C}^{n_\beta} \to \mathbb{C}^{n_\alpha} \otimes \mathbb{C}^{n_\beta}$. Here for each n, $I_n : \mathbb{C}^n \to \mathbb{C}^n$ is the identity map.
- The characteristic polynomial of operator $C_\alpha \otimes I_{n_\beta} + I_{n_\alpha} \otimes C_\beta$ is monic with integer coefficients.

The proof for $\alpha\beta$ is similar, except that here one considers $C_\alpha \otimes C_\beta : \mathbb{C}^{n_\alpha} \otimes \mathbb{C}^{n_\beta} \to \mathbb{C}^{n_\alpha} \otimes \mathbb{C}^{n_\beta}$.

Exercises

B.1 Show that $\sqrt{2} + \sqrt[3]{5}$ is an algebraic integer by explicitly finding the algebraic equation that this number satisfies.

B.2 Write the following polynomials in the terms of the basic symmetric functions:

a. $x^2 + y^2 + z^2$;
b. $x^3 + y^3 + z^3$;
c. $x^4 + y^4 + z^4$;
d. $(x - y)^2(y - z)^2(z - x)^2$.

B.3 Let α, β, γ be the three roots of the polynomial $x^3 + 7x^2 - 8x + 3$. Find the polynomial with rational coefficients whose roots are the following numbers:

a. $\alpha^2, \beta^2, \gamma^2$;
b. $1/\alpha, 1/\beta, 1/\gamma$;
c. $\alpha^3, \beta^3, \gamma^3$.

Appendix C
SageMath

SageMath is a free, open-source mathematical software which is a viable, powerful alternative to commercial computing packages such as Maple, or Mathematica. In this appendix we give a minimal introduction to SageMath. Bard's book [6], freely available online, is a good comprehensive introduction to the software with many examples. This book is our main reference for this appendix. Another useful reference for number theoretic applications of SageMath is Stein [49] where many numerical examples are worked out using SageMath.

SageMath is freely available for download from http://www.sagemath.org/. There are also two internet-based ways to use SageMath:

- SageMathCell is a web interface for SageMath, suitable for almost any everyday quick computation including all the computational exercises in this book. The website is https://sagecell.sagemath.org/
- CoCalc is a web service for online computation with the capability to support large volume computations, classroom support, etc., available at https://cocalc.com/

Here are some resources to get you started on SageMath. The online reference for SageMath is

www.sagemath.org/doc/reference

The online tutorial is available here

www.sagemath.org/doc/tutorial

A number of quick reference sheets containing very minimal lists of commands are available at

https://wiki.sagemath.org/quickref

To get acquainted with SageMath, the easiest way is to work within SageMathCell. This interface provides a window in which to type commands. There is also an `Evaluate` button to execute the commands (or one could press `Shift` and `Enter` at the same time).

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

C.1 Basic operations

To add numbers, one just types +, e.g., `2 + 3` gives `5`. Multiplication is `*`, `2*3` will evaluate to `6`, as it should. Power operation is written as `2^3`, which will give `8`. Division is more interesting: evaluating `4/5` gives `4/5`. In order to get the decimal expansion, one needs to enter `N(4/5)`, which returns `0.800000000000000`. Square root is similar. Evaluating `sqrt(8)` produces `2 * sqrt(2)`. Typing `N(sqrt(8))` and pressing `Evaluate` gives `2.82842712474619`. For other roots, one can type in

```
N(3^(1/6)).
```

For the exponential function one can try `exp(3)` or `e^ 3`, or for the numerical value `N(exp(3))`. Logarithms are also easy: `log(3)` returns the natural log of 3, whereas `log(3, 7)` gives the logarithm of 3 in base 7. Entering `sqrt(-4, all=true)` gives `[2*I , -2 *I]`, which means the list consisting of the complex numbers $2i$ and $-2i$. To try something a little more complicated one could try typing in

```
N(100*(1 + sqrt(2) + log(5, 62) )^5)
```

which immediately returns `17339.1704246701`. For more precision, one could type

```
N(100*(1 + sqrt(2) + log(5, 62) )^5, prec=200)
```

or

```
numerical_approx(100*(1 + sqrt(2) + log(5, 62) )^5,
digits=200)
```

which returns 200 digits.

SageMath can, very easily, plot functions. For example, `plot(3*exp(x+5))` plots the function $f(x) = 3e^{x+5}$ for $-1 < x < +1$. To get other ranges, e.g., $-3 < x < 5$, one types

```
plot(3*exp(x+5), -3, 5)
```

There are various other things one can do with `plot`, e.g., setting bounds in the y direction, superimposing graphs, etc., see [6, Ch. 3] for more details on plotting functions. One can also define functions. For example, one can define a function $f(x)$ by

```
f(x) = x^2 - 2
```

Next, evaluating `f(3)` returns `7`. One could also plot the function by typing `plot(f(x))`.

C.2 Basic number theory

Here we review some of the most basic number theoretic operations that SageMath can do.

Prime numbers

The command

```
primes_first_n(55)
```

lists the first 55 prime numbers:

```
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,
47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,
103, 107, 109, 113, 127, 131,  137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193,
197, 199, 211, 223, 227, 229, 233, 239, 241,
251, 257]
```

The command

```
is_prime(157)
```

checks the primality of 157, and returns `True`. Typing

```
next_prime(10057)
```

gives 10061 which is the next prime after 10057. There is also a similar command

```
previous_prime(10057)
```

The get the prime numbers in a certain range, e.g., 120 to 137, we use the command

```
prime_range(120, 137)
```

We get `[127, 131]` as the answer. If we need to find the 112th prime number, all we need to do is to type

```
nth_prime(112)
```

to see that that number is 613. Another useful command is

```
random_prime(10^20,10^30)
```

which returns a random prime number between 10^{20} and 10^{30}. Typing

```
prime_pi(x)
```

returns the number of prime numbers up to x.

Divisors

The command `factor` factorizes a number into a product of its prime factors, e.g., `factor(12)` gives

```
2^2 * 3
```

To get the list of divisors of a number we use the command `divisors`. For example `divisors(325)` gives the answer

```
[1, 5, 13, 25, 65, 325]
```

The function $\sigma_k(n) = \sum_{d|n} d^k$ is given by `sigma(n, k)`. For example, `sigma(325, 0)` simply counts the number of divisors of 325 and returns 6. The command `len(divisors(325))` would have done the same thing. The commands `gcd` and `lcm` compute gcd and lcm. For example, `gcd(12, 18)` returns 6, and `lcm(12, 18)` returns 36. The command `xgcd(a,b)` returns a triple (d, u, v) with $d = \gcd(a, b)$ and $au+bv = d$. For example, `xgcd(12,15)` gives `(3, -1, 1)`.

Modular arithmetic

Suppose we divide a by b, and we write $a = bq + r$. To find the remainder r of a when divided by b, one can type `a % b`. For example

```
329 % 162
```

returns 5. We could have alternatively used the command `mod(329, 162)` to get the same answer. To find the integer quotient q, we write $a//b$. For example, `329 // 162` gives 2. To find the modular inverse of the number 3 modulo 2005 we enter

```
inverse_mod(3, 2005).
```

The answer is 1337. One can verify this by checking that

```
(1337*3)%2005
```

in fact returns 1.

SageMath has the capability to do modular arithmetic. Suppose we want to compute the order of 5 modulo 7. In order to do this, we type

```
R = Integers(7)
a = R(5)
multiplicative_order(a)
```

This will produce 6 as the answer, which means that 5 is a primitive root modulo 7. One can check this by entering

```
[c^i for i in range(6)]
```

This last command produces `[1, 5, 4, 6, 2, 3]`.

An alternative way to do modular arithmetic is to use the `Mod` operator. For example, if we want to compute $2^{75} \mod 1000$, we can simply type

```
Mod(2, 1000)^75
```

which very quickly returns 568. To compute the multiplicative inverse we can execute the command

```
Mod(3, 1000)^(-1)
```

which produces 667.

The Chinese Remainder Theorem

A useful command is the Chinese Remainder Theorem command `CRT`. Entering `CRT(a, b, m, n)` finds an integer x such that

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n. \end{cases}$$

For example, `CRT(2, 1, 3, 5)` returns 11. If we have more than two congruence equations, we have to use

```
CRT_list([a_1, a_2, \dots, a_m], [n_1, n_2, \dots, n_m])
```

For example,

```
CRT_list([1, 2, 3], [5, 7, 9])
```

returns 156.

The Euler totient function

To calculate the Euler totient function of a number, e.g., 10032 we type in

```
euler_phi(10032)
```

to obtain 2880. SageMath can also find primitive roots. Typing

```
primitive_root(25)
```

returns 2 which is a primitive root modulo 25—in fact, this command returns the smallest primitive root modulo 25. If one enters

```
primitive_root(36)
```

the output will be the message `ValueError: no primitive root`.

Quadratic residues

SageMath has built-in functions to handle quadratic residues and related functions. For example,

```
quadratic_residues(7)
```

produces `[0, 1, 2, 4]` which is the list of quadratic residues modulo 7 plus 0. Note that this is different from our convention in Chapter 6 where a quadratic residue was defined to be coprime to p. The command for the Legendre symbol is

```
legendre_symbol(a, p)
```

For example,

```
legendre_symbol(3, 7)
```

gives -1. The command for the Jacobi symbol is

```
jacobi_symbol(a, n)
```

which works similar to the Legendre symbol.

Sums of squares

The command

```
two_squares(5)
```

returns `[1, 2]`, and $5 = 1^2 + 2^2$. The command

```
three_squares(6)
```

gives `[1, 1, 2]`. The command

```
four_squares(8)
```

produces `[0, 0, 2, 2]`.

C.3 Polynomial operations

Here we briefly explain how to work with polynomials in SageMath.

Polynomials over the real or complex numbers

Let us define the polynomials $a(x)$ and $b(x)$ by setting

```
a(x) = x^3 - 1
b(x) = x^2 - x - 2
```

Evaluating `a(2)` gives `7`. The command `a(x) + b(x)` returns

```
x^3 + x^2 - x - 3
```

Typing `a(x)*b(x)` gives

```
(x^3 - 1)*(x^2 - x - 2)
```

To do the multiplication one needs to enter `expand(a(x)*b(x))` which returns

```
x^5 - x^4 - 2*x^3 - x^2 + x + 2
```

The command `factor(a(x))` returns

```
(x^2 + x + 1)*(x - 1)
```

One can also compute the gcd of the polynomials by entering `gcd(a(x), b(x))` to obtain 1. Typing in `factor(lcm(a(x),b(x)))` gives

```
(x^2 + x + 1)*(x + 1)*(x - 1)*(x - 2)
```

To solve the equation `a(x)=0` one simply types `solve(a(x), x)`. The outcome is

```
[x == 1/2*I*sqrt(3) - 1/2, x == -1/2*I*sqrt(3) - 1/2,
x == 1]
```

The `solve` operator that we just introduced is a useful, versatile device that can be used in a variety of settings. For example, entering

```
var('z')
solve([a(x)-z==0, b(x)-2*z^2==5], x, z)
```

solves the system

$$\begin{cases} a(x) - z = 0, \\ b(x) - 2z^2 = 5. \end{cases}$$

The answer is

```
[[x == (1.214514354475611 + 0.4405103357723433*I),
z == (0.0844362836387264 + 1.863837112673745*I)],
[x == (1.214514354475611 - 0.4405103357723433*I),
z == (0.08443628363872642 - 1.863837112673745*I)],
 [x == (-0.9751234960329906 + 0.7411666213498296*I),
 z == (-0.3202238106249589 + 1.707106500754547*I)],
 [x == (-0.9751234960329906 - 0.7411666213498296*I),
 z == (-0.320223810624959 - 1.707106500754547*I)],
 [x == (-0.2393908584426201 + 1.319030559283378*I),
 z == (0.2357875269862346 - 2.068131317220872*I)],
 [x == (-0.2393908584426201 - 1.319030559283378*I),
 z == (0.2357875269862422 + 2.068131317220871*I)]]
```

Note that we did not have to declare the variable x as it is the default variable.

We refer the reader to the first chapter of [6] for other operations involving polynomials.

Polynomials modulo integers

We can specify the polynomial ring we work in using the command

```
R.<x> = PolynomialRing(Integers(7))
```

Then if we type

```
expand((3*x^2+5)*(2*x^3+3))
```

we obtain

```
6*x^5 + 3*x^3 + 2*x^2 + 1
```

If we type in

```
(x^3+1).roots()
```

we receive `[(6, 1), (5, 1), (3, 1)]` which lists the roots of x^3+1 in mod 7 numbers and their multiplicities. If we type

```
(3*x^2+5).roots()
```

we get `[]` in response which means the empty set, i.e., the polynomial $3x^2 + 5$ has no roots in mod 7 numbers.

Elliptic curves

In the Notes to Chapter 3 we defined a group law on the set of rational points on an elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$. The command

```
E = EllipticCurve([0, 17])
```

defines the elliptic curve $y^2 = x^3 + 0 \cdot x + 17$, and typing the command

```
E
```

returns

```
Elliptic Curve defined by y^2 = x^3 + 17 over Rational Field
```

We can also add points on elliptic curves:

```
A=E([-1, 4])
B=E([2,5])
A+B
```

will produce

```
(-8/9 : -109/27 : 1)
```

or

```
A+A
```

will give

```
(137/64 : -2651/512 : 1)
```

Note that the answers are always produced as triples $(a : b : c)$ considered in the *projective space* with $c = 0$ or 1. If $c = 0$, then the resulting point is the identity point of the elliptic curve group law, i.e., the point at infinity. SageMath can compute elliptic curve invariants such as *torsion subgroup* and *rank* but since we are not using those quantities in this book, we will not review them in this brief appendix.

SageMath is incredibly diverse, and this brief appendix is far from a satisfactory introduction. As mentioned at the beginning of this appendix, there are a variety of resources available on the web which one can use to look up commands. The wonderful thing about SageMath is that it is an open-source Python-based software, and one can do actual Python programming within the software. Also, SageMath is constantly growing thanks to a large group of individuals who have devoted many, many hours developing the code to perform various mathematical tasks. And if anyone realizes that there is something that SageMath is missing, they can get involved in the effort.

References

1. Ahlfors, Lars V. *Complex analysis: An introduction of the theory of analytic functions of one complex variable*. Second edition McGraw-Hill Book Co., New York-Toronto-London 1966 xiii+317 pp.
2. Apostol, Tom M. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer, New York-Heidelberg, 1976. xii+338 pp.
3. Aristotle, *Prior Analytics*. Book I. Translated with an introduction and commentary by Gisela Striker. Oxford Univdersity Press. 2009.
4. Artin, Emil, *The gamma function*. Translated by Michael Butler. Athena Series: Selected Topics in Mathematics Holt, Rinehart and Winston, New York-Toronto-London 1964 vii+39 pp.
5. Artmann, Benno. *Euclid—the creation of mathematics*. Springer, New York, 1999. xvi+343 pp.
6. G. Bard, *Sage for Undergraduates*, American Mathematical Society, available for download at http://bookstore.ams.org/mbk-87/
7. Berndt, Bruce C.; Evans, Ronald J.; Williams, Kenneth S. Gauss and Jacobi sums. Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York, 1998. xii+583 pp.
8. Borevich, A. I.; Shafarevich, I. R. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966 x+435 pp.
9. Burton, David M. *The history of mathematics. An introduction*. Second edition. W. C. Brown Publishers, Dubuque, IA, 1991. xii+678 pp.
10. Carmichael, Robert, *Diophantine Analysis*, First edition. John Wiley and Sons. 1915.
11. Cassels, J. W. S. *An introduction to the geometry of numbers*. Corrected reprint of the 1971 edition. Classics in Mathematics. Springer, Berlin, 1997. viii+344 pp.
12. Cassels, J. W. S. *Rational quadratic forms*. London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. xvi+413 pp.
13. Conway, John H.; Smith, Derek A. On quaternions and octonions: their geometry, arithmetic, and symmetry. A K Peters, Ltd., Natick, MA, 2003. xii+159 pp.
14. Cox, David A., *Primes of the form* $x^2 + ny^2$. Fermat, class field theory, and complex multiplication. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013. xviii+356 pp.
15. Dickson, Leonard Eugene. *History of the theory of numbers. Vol. I: Divisibility and Primality*, Carnegie Institute of Washington, 1919.

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

16. Dickson, Leonard Eugene. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York 1966 xxv+803 pp.
17. Dumbaugh, Della; Schwermer, Joachim. *Emil Artin and beyond—class field theory and L-functions.* With contributions by James Cogdell and Robert Langlands. Heritage of European Mathematics. European Mathematical Society (EMS), Zrich, 2015. xiv+231 pp.
18. Ebbinghaus, H.-D.; Hermes, H.; Hirzebruch, F.; Koecher, M.; Mainzer, K.; Neukirch, J.; Prestel, A.; Remmert, R. *Numbers*. With an introduction by K. Lamotke. Translated from the second 1988 German edition by H. L. S. Orde. Translation edited and with a preface by J. H. Ewing. Graduate Texts in Mathematics, 123. Readings in Mathematics. Springer, New York, 1991. xviii+395 pp.
19. Edwards, Harold M. *Fermat's last theorem. A genetic introduction to algebraic number theory*. Corrected reprint of the 1977 original. Graduate Texts in Mathematics, 50. Springer, New York, 1996. xvi+410 pp.
20. Euclid. *Elements. All thirteen books complete in one volume.* The Thomas L. Heath translation. Edited by Dana Densmore. Green Lion Press, Santa Fe, NM, 2002. xxx+499 pp.
21. Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer, New York, 1986. xx+472 pp.
22. Equidistribution in number theory, an introduction. Proceedings of the NATO Advanced Study Institute (the 44th Sminaire de Mathmatiques Suprieures (SMS)) held at the Universit de Montral, Montral, QC, July 11–22, 2005. Edited by Andrew Granville and Zev Rudnick. NATO Science Series II: Mathematics, Physics and Chemistry, 237. Springer, Dordrecht, 2007. xvi+345 pp.
23. Guy, Richard K. *Unsolved problems in number theory*. Third edition. Problem Books in Mathematics. Springer, New York, 2004. xviii+437 pp.
24. Hardy, G. H.; Wright, E. M. *An introduction to the theory of numbers*. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp.
25. Herstein, I. N. *Topics in algebra*. Second edition. Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975. xi+388 pp.
26. Hilbert, David. *Foundations of geometry*. Second edition. Translated from the tenth German edition by Leo Unger Open Court, LaSalle, Ill. 1971 ix+226 pp.
27. Jacobson, Michael J., Jr.; Williams, Hugh C. *Solving the Pell equation*. CMS Books in Mathematics/Ouvrages de Mathmatiques de la SMC. Springer, New York, 2009. xx+495 pp.
28. Joseph, G. G., *Crest of the Peacock: Non-European Roots of Mathematics*, Third Edition, Princeton University Press, 2011.
29. Kline, Morris, *Mathematical Thought from Ancient to Modern*, Vol 1, Oxford University Press, 1990.
30. Koblitz, Neal. *Introduction to elliptic curves and modular forms.* Second edition. Graduate Texts in Mathematics, 97. Springer, New York, 1993. x+248 pp.
31. Landau, Edmund. *Elementary number theory.* Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958. 256 pp.
32. Lemmermeyer, Franz, *Reciprocity laws. From Euler to Eisenstein.* Springer Monographs in Mathematics. Springer, Berlin, 2000. xx+487 pp.
33. Miller, Steven J.; Takloo-Bighash, Ramin. *An invitation to modern number theory*. With a foreword by Peter Sarnak. Princeton University Press, Princeton, NJ, 2006. xx+503 pp.
34. G. H. Mossaheb, *Elementary Theory of Numbers* (in Persian), Vol 2, Soroush, Tehran. 1979. 1803 pp.
35. Murty, M. Ram. *Problems in analytic number theory*. Second edition. Graduate Texts in Mathematics, 206. Readings in Mathematics. Springer, New York, 2008. xxii+502 pp.
36. Mozzochi, C. J. *The Fermat diary.* American Mathematical Society, Providence, RI, 2000. xii+196 pp.
37. Murty, M. Ram; Esmonde, Jody. *Problems in algebraic number theory*. Second edition. Graduate Texts in Mathematics, 190. Springer, New York, 2005. xvi+352 pp.

38. Jowell, B. *The Dialogues of Plato, with analyses and introductions*, Vol IV. Oxford University Press, 1892.
39. Plofker, Kim, *Mathematics in India*, Princeton University Press, 2009.
40. Rashed, R. *Encyclopedia of the History of Arabic Science*, Vol 2.
41. Rudin, Walter. *Principles of mathematical analysis*. Third edition. International Series in Pure and Applied Mathematics. McGraw-Hill Book Co., New York-Auckland-Düsseldorf, 1976. x+342 pp.
42. Russell, Bertrand. *A history of western philosophy, and its connection with political and social circumstances from the earliest times to the present day.* New York, Simon and Schuster, 1945. xxiii+895 pp.
43. Samuel, Pierre. *Algebraic theory of numbers.* Translated from the French by Allan J. Silberger Houghton Mifflin Co., Boston, Mass. 1970, 109 pp.
44. Serre, J.-P., *A course in arithmetic*. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer, New York-Heidelberg, 1973. viii+115 pp.
45. Siegel, Carl Ludwig *Lectures on the geometry of numbers.* Notes by B. Friedman. Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter. With a preface by Chandrasekharan. Springer, Berlin, 1989. x+160 pp.
46. Sierpiński, W. *Elementary theory of numbers*. Second edition. Edited and with a preface by Andrzej Schinzel. North-Holland Mathematical Library, 31. North-Holland Publishing Co., Amsterdam; PWN—Polish Scientific Publishers, Warsaw, 1988. xii+515 pp.
47. Silverman, Joseph H. *The arithmetic of elliptic curves*. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer, New York, 1992. xii+400 pp.
48. Silverman, Joseph H.; Tate, John T. *Rational points on elliptic curves*. Second edition. Undergraduate Texts in Mathematics. Springer, Cham, 2015. xxii+332 pp.
49. Stein, William, *Elementary number theory: primes, congruences, and secrets.* A computational approach. Undergraduate Texts in Mathematics. Springer, New York, 2009. x+166 pp.
50. Stewart, Ian; Tall, David, *Algebraic number theory and Fermat's last theorem.* Fourth edition. CRC Press, Boca Raton, FL, 2016. xix+322 pp.
51. Thomas, I. *Selections Illustrating the history of Greek Mathematics*, Vol. I. From Thales to Euclid. xvi+505 pp. Vol. II. From Aristarchus to Pappus. x+683 pp. Harvard University Press, Cambridge, Mass.; William Heinemann, Ltd., London, 1951.
52. Titchmarsh, E. C. *The theory of the Riemann zeta-function.* Second edition. Edited and with a preface by D. R. Heath-Brown. The Clarendon Press, Oxford University Press, New York, 1986. x+412 pp.
53. Trappe, Wade; Washington, Lawrence C., *Introduction to cryptography with coding theory.* Second edition. Pearson Prentice Hall, Upper Saddle River, NJ, 2006. xiv+577 pp.
54. Vaughan, R. C. *The Hardy-Littlewood method*. Second edition. Cambridge Tracts in Mathematics, 125. Cambridge University Press, Cambridge, 1997. xiv+232 pp.
55. van der Waerden, B. L. *Geometry and Algebra in Ancient Civiliazations*, Springer, 1983.
56. Weil, André. *Basic number theory*. Reprint of the second (1973) edition. Classics in Mathematics. Springer, Berlin, 1995. xviii+315 pp.
57. Weil, André. *Number theory. An approach through history from Hammurapi to Legendre*. Reprint of the 1984 edition. Modern Birkhuser Classics. Birkhuser Boston, Inc., Boston, MA, 2007. xxii+377 pp.
58. Agrawal, M., Kayal, N., and Saxena, N. *PRIMES is in P*. Annals of Mathematics 160(2), 2004, 781–793.
59. Alter, Ronald; Curtz, Thaddeus B.; Kubota, K. K. *Remarks and results on congruent numbers*. Proceedings of the Third Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1972), pp. 27–35. Florida Atlantic Univ., Boca Raton, Fla., 1972.
60. Alter, Ronald; Curtz, Thaddeus B. *A note on congruent numbers*. Math. Comp. 28 (1974), 303-305.
61. Ankeny, N. C. *Sums of three squares*. Proc. Amer. Math. Soc. 8 (1957), 316-319.

62. Baez, John C. The octonions. Bull. Amer. Math. Soc. (N.S.) 39 (2002), no. 2, 145-205.
63. Baker, Alan. *Experiments on the abc-conjecture*, Publ. Math. Debrecen, 65 (2004), pp. 253–260.
64. Chapman, R., *Evaluating* $\zeta(2)$, http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf.
65. Chen, J.R. *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*. Sci. Sinica 16 (1973), 157–176.
66. Cilleruelo, J., *The distribution of the lattice points on circles*, Journal of Number Theory, 43, 198–202 (1993).
67. Cilleruelo, J.; Córdoba, A. *Trigonometric polynomials and lattice points*. Proc. Amer. Math. Soc. 115 (1992), no. 4, 899-905.
68. Cilleruelo, Javier; Granville, Andrew, *Lattice points on circles, squares in arithmetic progressions and sumsets of squares*. Additive combinatorics, 241–262, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.
69. Conrad, K., *The Gaussian Integers*, available at http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf
70. Conrad, K., *The Congruent Number Problem*, available at http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf
71. Davenport, H. *The geometry of numbers*. Math. Gaz. 31, (1947). 206–210.
72. Duke, W. *Rational points on the sphere*. Rankin memorial issues. Ramanujan J. 7 (2003), no. 1-3, 235–239.
73. Erdös, P. *On sets of distances of n points in Euclidean space*. Magyar Tud. Akad. Mat. Kutató Int. Közl. 5 (1960) 165–169, available at http://www.renyi.hu/~p_erdos/1960-08.pdf
74. Estermann, T. *On the representations of a number as a sum of squares*, Prace Matematyczno-Fizyczne (1937) Volume: 45, Issue: 1, page 93–125.
75. Gelbart, Stephen, *An elementary introduction to the Langlands program*. Bull. Amer. Math. Soc. (N.S.) 10 (1984), no. 2, 177–219.
76. Goldston, Daniel A.; Pintz, János; Yıldırım, Cem Y. *Primes in tuples. I*. Ann. of Math. (2) 170 (2009), no. 2, 819–862.
77. Granville, Andrew; Tucker, Thomas J. *It's as easy as abc*. Notices Amer. Math. Soc. 49 (2002), no. 10, 1224–1231.
78. Gross, Benedict H. *The work of Manjul Bhargava*. Proceedings of the International Congress of Mathematicians–Seoul 2014. Vol. 1, 56–63, Kyung Moon Sa, Seoul, 2014.
79. Hardy, G. H. *On the representation of a number as the sum of any number of squares, and in particular of five*. Trans. Amer. Math. Soc. 21 (1920), no. 3, 255–284.
80. Hirschhorn, M. D. *A simple proof of Jacobi's four-square theorem*. Proc. Amer. Math. Soc. 101 (1987), no. 3, 436–438.
81. Hooley, C. *Artin's conjecture for primitive roots*, J. Reine Angew. Math. 225 (1967), 209–220.
82. Laishram, Shanta. *Baker's explicit abc-conjecture and Waring's problem*. Hardy-Ramanujan J. 38 (2015), 49–52.
83. Lehmer, Derrick Norman; Asymptotic Evaluation of Certain Totient Sums. Amer. J. Math. 22 (1900), no. 4, 293–335.
84. Brillhart, John. *Emma Lehmer 1906–2007*. Notices Amer. Math. Soc. 54 (2007), no. 11, 1500–1501.
85. Maynard, James. *Small gaps between primes*. Ann. of Math. (2) 181 (2015), no. 1, 383–413.
86. Mazur, B. *Number theory as gadfly*. Amer. Math. Monthly 98 (1991), no. 7, 593–610.
87. Michel, Philippe; Venkatesh, Akshay, *Equidistribution, L-functions and ergodic theory: on some problems of Yu. Linnik*. International Congress of Mathematicians. Vol. II, 421–457, Eur. Math. Soc., Zrich, 2006.
88. Moree, Pieter. *Artin's primitive root conjecture: a survey*. Integers 12 (2012), no. 6, 1305–1416.
89. Murty, M. Ram. *Artin's conjecture for primitive roots*. Math. Intelligencer 10 (1988), no. 4, 59–67.

90. Pieper, Herbert, *On Euler's contributions to the four-squares theorem*. Historia Math. 20 (1993), no. 1, 12–18.
91. Polymath, D. H. J. *Variants of the Selberg sieve, and bounded intervals containing many primes*. Res. Math. Sci. 1 (2014), Art. 12, 83 pp.
92. Rice, Adrian; Brown, Ezra. *Why ellipses are not elliptic curves*. Math. Mag. 85 (2012), no. 3, 163–176.
93. Riemann, B. *On the Number of Prime Numbers less than a Given Quantity*. Translated from German by David R. Wilkins. Available at http://www.claymath.org/sites/default/files/ezeta.pdf
94. Rousseau, G. *On the quadratic reciprocity law*. J. Austral. Math. Soc. Ser. A 51 (1991), no. 3, 423–425.
95. Smith, Alexander, *The congruence numbers have positive natural density*, preprint.
96. Smith, Alexander, 2^∞*-Selmer groups*, 2^∞*-class groups, and Goldfeld's conjecture*, preprint.
97. Stephens, N. M. *Congruence properties of congruent numbers*. Bull. London Math. Soc. 7 (1975), 182–184.
98. Soundararajan, K. *Small gaps between prime numbers: the work of Goldston-Pintz-Y?ld?r?m*. Bull. Amer. Math. Soc. (N.S.) 44 (2007), no. 1, 1–18.
99. Sullivan, W. R., *Numerous proofs of* $\zeta(2) = \frac{\pi^2}{6}$, http://math.cmu.edu/~bwsulliv/MathGradTalkZeta2.pdf.
100. Takloo-Bighash, Ramin. *Distribution of rational points: a survey*. Bull. Iranian Math. Soc. 35 (2009), no. 1, 1–30.
101. Tian, Ye. *Congruent numbers and Heegner points*. Camb. J. Math. 2 (2014), no. 1, 117–161.
102. Tian, Y., Yuan, X., and Zhang, S.-W. *Genus Periods, Genus Points and Congruent Number Problem*, To appear in Asia J. Math.
103. Trainin, J. *An elementary proof of Pick's theorem*, The Mathematical Gazette, Vol. 91, No. 522 (2007), pp. 536–540.
104. Tschinkel, Yuri, *Algebraic varieties with many rational points*. Arithmetic geometry, 243–334, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009.
105. Tunnell, J. B. *A classical Diophantine problem and modular forms of weight 3/2*. Invent. Math. 72 (1983), no. 2, 323–334.
106. Vaughan, R. C.; Wooley, T. D. *Waring's problem: a survey*. Number theory for the millennium, III (Urbana, IL, 2000), 301–340, A K Peters, Natick, MA, 2002.
107. Waldschmidt, Michel. *Lecture on the abc conjecture and some of its consequences*. Mathematics in the 21st century, 211–230, Springer Proc. Math. Stat., 98, Springer, Basel, 2015.
108. Weil, André. *Numbers of solutions of equations in finite fields*. Bull. Amer. Math. Soc. 55, (1949). 497–508.
109. Weil, André. *Prehistory of the zeta-function*. Number theory, trace formulas and discrete groups (Oslo, 1987), 1–9, Academic Press, Boston, MA, 1989.
110. Wiles, Andrew, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141 (1995), no. 3, 443–551.
111. Wooley, T. D. *On Waring's problems for intermediate powers*, https://arxiv.org/pdf/1602.03221.pdf
112. Zhang, Yitang. *Bounded gaps between primes*. Ann. of Math. (2) 179 (2014), no. 3, 1121–1174.
113. http://mathoverflow.net/questions/217698/many-representations-as-a-sum-of-three-squares
114. NOVA, The proof, http://www.pbs.org/wgbh/nova/proof/

Index

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