Math 784: algebraic NUMBER THEORY
(Instructor's Notes)*

Algebraic Number Theory:

• What is it? The goals of the subject include: (i) to use algebraic concepts to deduce information about integers and other rational numbers and (ii) to investigate generalizations of the integers and rational numbers and develop theorems of a more general nature. Although (ii) is certainly of interest, our main point of view for this course will be (i). The focus of this course then will be on the use of algebra as a tool for obtaining information about integers and rational numbers.

• A simple example. Here, we obtain as a consequence of some simple algebra the following:

Theorem 1. *Let $\theta \in \mathbb{Q}$ with $0 \le \theta \le 1/2$. Then $\sin^2(\pi\theta) \in \mathbb{Q}$ if and only if $\theta \in \{0, 1/6, 1/4, 1/3, 1/2\}$.*

It is easy to check that for $\theta \in \{0, 1/6, 1/4, 1/3, 1/2\}$, we have $\sin^2(\pi\theta)$ is rational; so we are left with establishing that if $\sin^2(\pi\theta) \in \mathbb{Q}$, then $\theta \in \{0, 1/6, 1/4, 1/3, 1/2\}$. Observe that we can use Theorem 1 to immediately determine for what $\theta \in \mathbb{Q}$ the value of $\sin(\pi\theta)$ is rational (see the upcoming homework assignment). Before getting to the proof of this theorem, we give some background.

• Some definitions and preliminaries.

Definition. Let α be a complex number. Then α is *algebraic* if it is a root of some $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$. Otherwise, α is *transcendental*.

Examples and Comments:

(1) Rational numbers are algebraic.
(2) The number $i = \sqrt{-1}$ is algebraic.
(3) The numbers π, e, and e^π are transcendental.
(4) The status of π^e is unknown.
(5) Almost all numbers are transcendental.

Definition. An algebraic number α is an *algebraic integer* if it is a root of some monic polynomial $f(x) \in \mathbb{Z}[x]$ (i.e., a polynomial $f(x)$ with integer coefficients and leading coefficient one).

Examples and Comments:

(1) Integers (sometimes called "rational integers") are algebraic integers.
(2) Rational numbers which are not rational integers are not algebraic integers. In other words, we have

*These notes are from a course taught by Michael Filaseta in the Spring of 1997 and 1999 but based on notes from previous semesters.

Theorem 2. *If α is a rational number which is also an algebraic integer, then $\alpha \in \mathbb{Z}$.*

Proof. Suppose $f(a/b) = 0$ where $f(x) = \sum_{j=0}^{n} a_j x^j$ with $a_n = 1$ and where a and b are relatively prime integers with $b > 0$. It suffices to show $b = 1$. From $f(a/b) = 0$, it follows that

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0.$$

It follows that a^n has b as a factor. Since $\gcd(a, b) = 1$ and $b > 0$, we deduce that $b = 1$, completing the proof. ■

(3) The number i is an algebraic integer.
(4) Transcendental numbers are not algebraic integers.
(5) If $u \in \mathbb{Q}$, then $2\cos(\pi u)$ is an algebraic integer. This requires an explanation which we supply next.

Lemma. *For each positive integer m, there is a $g_m(x) = \sum_{j=0}^{m} b_j x^j \in \mathbb{Z}[x]$ satisfying:*
(i) $\cos(m\theta) = g_m(\cos\theta)$
(ii) $b_m = 2^{m-1}$
(iii) $2^{k-1} | b_k$ *for* $k \in \{2, 3, \ldots, m\}$.

Proof. We do induction on m. The cases $m = 1$ and $m = 2$ are easily checked. Suppose the lemma holds for $m \le n$. Observe that

$$\cos((n+1)\theta) + \cos((n-1)\theta) = 2\cos(n\theta)\cos\theta.$$

Then (i), (ii), and (iii) follow by considering $g_{n+1}(x) = 2x g_n(x) - g_{n-1}(x)$. ■

Write $u = a/m$ with m a positive integer. By the lemma,

$$\pm 1 = \cos(m\pi u) = g_m(\cos(\pi u)) = \sum_{j=0}^{m} b_j (\cos(\pi u))^j,$$

where $b_m = 2^{m-1}$ and for some integers b'_j we have $b_j = 2^{j-1} b'_j$ for $j \in \{2, 3, \ldots, m-1\}$. Multiplying through by 2 and rearranging, we deduce that $2\cos(\pi u)$ is a root of

$$x^m + b'_{m-1}x^{m-1} + \cdots + b'_2 x^2 + b_1 x + (2b_0 \mp 2).$$

It follows that $2\cos(\pi u)$ is an algebraic integer.

• An application. Before proving Theorem 1, we determine for what $\theta \in \mathbb{Q}$, the value of $\cos(\pi\theta)$ is rational. By the last example above, if $\theta \in \mathbb{Q}$, then $2\cos(\pi\theta)$ is an algebraic integer. If we also have $\cos(\pi\theta)$ is rational, then Theorem 2 implies that $2\cos(\pi\theta) \in \mathbb{Z}$. Since $|2\cos(\pi\theta)| \le 2$, we deduce that $2\cos(\pi\theta) \in \{-2, -1, 0, 1, 2\}$ so that $\cos(\pi\theta) \in \{-1, -1/2, 0, 1/2, 1\}$. It follows that both θ and $\cos(\pi\theta)$ are rational if and only if $\theta \in \{k/2 : k \in \mathbb{Z}\} \cup \{k/3 : k \in \mathbb{Z}\}$.

• Completing the proof of Theorem 1. Let $u = 2\theta$, and suppose that $\sin^2(\pi\theta) \in \mathbb{Q}$. Then $2\cos(\pi u) = 2 - 4\sin^2(\pi\theta)$ is an algebraic integer which is also rational. By Theorem

2, we deduce $2 - 4\sin^2(\pi\theta) \in \mathbb{Z}$. It follows that $4\sin^2(\pi\theta)$ is a non-negative rational integer which is ≤ 4. We deduce that $\sin^2(\pi\theta) \in \{0, 1/4, 1/2, 3/4, 1\}$. Note that $\sin(\pi x)$ is a positive increasing function for $0 \le x \le 1/2$ so that there can be no more than 5 such θ. The result easily follows. (Note that the previous application involving $\cos(\pi\theta)$ could have been used to prove Theorem 1.)

Homework:

(1) Prove that $\sin(1^\circ)$ is algebraic. (One approach is to begin by showing that the coefficient of x^j in $g_m(x)$, as given in the lemma, is 0 if $j \not\equiv m \pmod 2$. There are easier approaches, but I won't give hints for them.)

(2) (a) Using Theorem 1, determine the values of $\theta \in \mathbb{Q} \cap [0, 2)$ for which $\sin^2(\pi\theta) \in \mathbb{Q}$.
(b) Using Theorem 1, determine the values of $\theta \in \mathbb{Q} \cap [0, 2)$ for which $\sin(\pi\theta) \in \mathbb{Q}$.

(3) Determine explicitly the set S satisfying: both $\theta \in [0, 1/2]$ and $\cos^2(\pi\theta)$ are rational if and only if $\theta \in S$.

(4) Let n denote a positive integer. Prove that $\dfrac{1}{\pi}\cos^{-1}\left(\dfrac{1}{\sqrt{n}}\right)$ is rational if and only if $n \in \{1, 2, 4\}$.

(5) Using Theorem 2, prove that if m is a positive integer for which $\sqrt{m} \in \mathbb{Q}$, then m is a square (i.e., $m = k^2$ for some $k \in \mathbb{Z}$).

The Elementary Symmetric Functions:

- The definition. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be n variables. Then

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n \\
\sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \\
\sigma_3 &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\
\vdots \quad & \quad \vdots \\
\sigma_n &= \alpha_1\alpha_2\cdots\alpha_n
\end{aligned}$$

are the elementary symmetric functions in $\alpha_1, \alpha_2, \ldots, \alpha_n$.

- Why the terminology? The term "symmetric" refers to the fact that if we permute the α_j in any manner, then the values of $\sigma_1, \ldots, \sigma_n$ remain unchanged. More explicitly, a function $f(\alpha_1, \ldots, \alpha_n)$ is symmetric in $\alpha_1, \ldots, \alpha_n$ if for all $\phi \in S_n$ (the symmetric group on $\{1, 2, \ldots, n\}$), we have $f(\alpha_{\phi(1)}, \ldots, \alpha_{\phi(n)}) = f(\alpha_1, \ldots, \alpha_n)$. The term "elementary" refers to the following:

Theorem 3. *Let R be a commutative ring with an identity. Then every symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ with coefficients in R is expressible as a polynomial in $\sigma_1, \ldots, \sigma_n$ with coefficients in R.*

Proof. For a symmetric $h(\alpha_1, \ldots, \alpha_n) \in R[\alpha_1, \ldots, \alpha_n]$, we set $T = T_h$ to be the set of n-tuples $(\ell_1, \ldots, \ell_n)$ with the coefficient of $\alpha_1^{\ell_1} \cdots \alpha_n^{\ell_n}$ in $h(\alpha_1, \ldots, \alpha_n)$ non-zero. We define the *size* of h to be $(k_1, \dots, k_n)$ where $(k_1, \dots, k_n)$ is the element of T with k_1 as large as possible, k_2 as large as possible given k_1, etc. Since $h(\alpha_1, \dots, \alpha_n)$ is symmetric, it follows that $(\ell_1, \dots, \ell_n) \in T$ if and only if each permutation of $(\ell_1, \dots, \ell_n)$ is in T. This implies that $k_1 \geq k_2 \geq \cdots \geq k_n$. Observe that we can use the notion of size to form an ordering on the elements of $R[\alpha_1, \dots, \alpha_n]$ in the sense that if h_1 has size $(k_1, \dots, k_n)$ and h_2 has size $(k'_1, \dots, k'_n)$, then $h_1 > h_2$ if there is an $i \in \{0, 1, \dots, n-1\}$ such that $k_1 = k'_1, \dots, k_i = k'_i$, and $k_{i+1} > k'_{i+1}$. Note that the elements of $R[\alpha_1, \dots, \alpha_n]$ which have size $(0, 0, \dots, 0)$ are precisely the constants (the elements of R).

Suppose now that $(k_1, \dots, k_n)$ represents the size of some symmetric $g \in R[\alpha_1, \dots, \alpha_n]$ with $g \notin R$. For non-negative integers $d_1, \dots, d_n$, the size of $h = \sigma_1^{d_1} \sigma_2^{d_2} \cdots \sigma_n^{d_n}$ is $(d_1 + d_2 + \cdots + d_n, d_2 + \cdots + d_n, \dots, d_{n-1} + d_n, d_n)$. Taking $d_1 = k_1 - k_2, d_2 = k_2 - k_3, \dots, d_{n-1} = k_{n-1} - k_n$, and $d_n = k_n$, we get the size of h is $(k_1, \dots, k_n)$. The coefficient of $\alpha_1^{k_1} \cdots \alpha_n^{k_n}$ in h is 1. It follows that there is an $a \in R$ such that $g - ah$ is of smaller size than g.

The above implies that for any symmetric element $f \in R[\alpha_1, \dots, \alpha_n]$, there exist $a_1, \dots, a_m \in R$ and $h_1, \dots, h_m \in R[\sigma_1, \dots, \sigma_n]$ such that $f - a_1 h_1 - \cdots - a_m h_m$ has size $(0, 0, \dots, 0)$. This implies the theorem. ■

• Elementary symmetric functions on roots of polynomials. Let $f(x) = \sum_{j=0}^{n} a_j x^j$ be a non-zero polynomial in $\mathbb{C}[x]$ of degree n with not necessarily distinct roots $\alpha_1, \dots, \alpha_n$. Then it is easy to see that

$$f(x) = a_n \prod_{j=1}^{n} (x - \alpha_j) = a_n x^n - a_n \sigma_1 x^{n-1} + a_n \sigma_2 x^{n-2} + \cdots + (-1)^n a_n \sigma_n,$$

where now we view the σ_j as elementary symmetric functions in the numbers $\alpha_1, \dots, \alpha_n$. It follows that

$$(*) \qquad \sigma_1 = -\frac{a_{n-1}}{a_n}, \ \sigma_2 = \frac{a_{n-2}}{a_n}, \ \dots, \ \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

• An example (almost Putnam Problem A-1 from 1976). Consider all lines which pass through the graph of $y = 2x^4 + 7x^3 + 3x - 5$ in 4 distinct points, say (x_j, y_j) for $j = 1, 2, 3, 4$. We will show that the average of the x_j's is independent of the line and find its value.

If $y = mx + b$ intersects $y = 2x^4 + 7x^3 + 3x - 5$ as indicated, then $x_1, \dots, x_4$ must be the four distinct roots of $2x^4 + 7x^3 + (3 - m)x - (b + 5) = 0$. From the previous section, we deduce that the sum of the x_j's is $\sigma_1 = -7/2$. The average of the x_j's is therefore $-7/8$.

Homework:

(1) Show that the average of the x_j^2's is independent of the line and find its value.

(2) Prove or disprove that the average of the y_j's is independent of the line.

(3) In the proof of Theorem 3, we deduced that the size of $g - ah$ is smaller than the size of g. By continuing the process, we claimed that eventually we would obtain an element of $R[\alpha_1, \dots, \alpha_n]$ of size $(0, 0, \dots, 0)$. Prove this as follows. Explain why the claim is true if $n = 1$. Consider $n \geq 2$. Let $(k_1, \dots, k_n)$ be the size of g with $g \notin R$, and let $(k'_1, \dots, k'_n)$

be the size of $g - ah$. Let b be an integer $\ge k_1$. Associate the integer $\sum_{j=0}^{n-1} \ell_{n-j} b^j$ with an n-tuple $(\ell_1, \dots, \ell_n)$. Show that the integer associated with $(k_1, \dots, k_n)$ is greater than the integer associated with $(k_1', \dots, k_n')$. Explain why $(0, 0, \dots, 0)$ is obtained by continuing the process as claimed. (There are other approaches to establishing that $(0, 0, \dots, 0)$ will be obtained, and you can feel free to establish this in a different manner.)

Algebraic Numbers and Algebraic Integers as Algebraic Structures:

- The main theorems we deal with here are as follows.

Theorem 4. *The algebraic numbers form a field.*

Theorem 5. *The algebraic integers form a ring.*

To prove these, we suppose that α and β are algebraic numbers or integers, and prove that $-\alpha$, $\alpha + \beta$, and $\alpha\beta$ are likewise. In the case that α is a non-zero algebraic number, we show that $1/\alpha$ is as well.

- The case for $-\alpha$. If $f(x)$ is a polynomial with integer coefficients having α as a root, then we consider $\pm f(-x)$. If $f(x)$ is monic, then one of these will be as well. Hence, if α is an algebraic number, then so is $-\alpha$; and if α is an algebraic integer, then so is $-\alpha$.

- The case for $\alpha + \beta$. Suppose α is a root of $f(x) \in \mathbb{Z}[x]$ and β is a root of $g(x) \in \mathbb{Z}[x]$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ denote the complete set of roots of $f(x)$ (counted to their multiplicity so that the degree of $f(x)$ is n) and let $\beta_1 = \beta, \beta_2, \dots, \beta_m$ denote the complete set of roots of $g(x)$. Consider the polynomial

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \big(x - (\alpha_i + \beta_j)\big).$$

Taking $R = \mathbb{Z}[\beta_1, \dots, \beta_m]$ in Theorem 3, we see that the coefficients of $F(x)$ are symmetric polynomials in $\alpha_1, \dots, \alpha_n$. Thus, if $\sigma_1, \dots, \sigma_n$ correspond to the elementary symmetric functions in $\alpha_1, \dots, \alpha_n$ and A is some coefficient (of x^k) in $F(x)$, then $A = B(\sigma_1, \dots, \sigma_n, \beta_1, \dots, \beta_m)$ for some polynomial B with integer coefficients. Now, the coefficients of $F(x)$ are also symmetric in $\beta_1, \dots, \beta_m$. Taking $R = \mathbb{Z}[\sigma_1, \dots, \sigma_n]$ in Theorem 3 and $\sigma_1', \dots, \sigma_m'$ to be the elementary symmetric functions in $\beta_1, \dots, \beta_m$, we get that $A = B'(\sigma_1, \dots, \sigma_n, \sigma_1', \dots, \sigma_m')$ for some polynomial B' with integer coefficients. On the other hand, $(*)$ implies that $\sigma_1, \dots, \sigma_n, \sigma_1', \dots, \sigma_m'$ are all rational so that $A \in \mathbb{Q}$. Thus, $F(x) \in \mathbb{Q}[x]$ and $m'F(x) \in \mathbb{Z}[x]$ for some integer m'. Since $\alpha + \beta$ is a root of $m'F(x)$, we deduce that $\alpha + \beta$ is an algebraic number. If α and β are algebraic integers, then we can take the leading coefficients of $f(x)$ and $g(x)$ to be 1 so that $(*)$ implies that each of $\sigma_1, \dots, \sigma_n, \sigma_1', \dots, \sigma_m'$ is in $\mathbb{Z}$ so that $F(x) \in \mathbb{Z}[x]$. Since $F(x)$ is monic, we obtain that in this case $\alpha + \beta$ is an algebraic integer.

- The case for $\alpha\beta$. The same idea as above works to show $\alpha\beta$ is an algebraic number (or integer) by defining

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \big(x - \alpha_i \beta_j\big).$$

• The case for $1/\alpha$. Suppose $\alpha \neq 0$ and α is a root of $\sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$. Then it is easy to show that $1/\alpha$ is a root of $\sum_{j=0}^{n} a_{n-j} x^j \in \mathbb{Z}[x]$. Hence, $1/\alpha$ is an algebraic number.

Comments: The above completes the proofs of Theorems 4 and 5. Suppose α is a non-zero algebraic integer. We note that $1/\alpha$ is an algebraic integer if and only if α is a root of a monic polynomial in $\mathbb{Z}[x]$ with constant term ± 1.

• An additional result. Next, we prove the following:

Theorem 6. *If α is an algebraic number, then there is a positive rational integer d such that $d\alpha$ is an algebraic integer.*

Proof. Suppose α is a root of $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_n \neq 0$. By considering $-f(x)$ if necessary, we may suppose $a_n > 0$. Since α is a root of $a_n^{n-1} f(x) = \sum_{j=0}^{n} a_j a_n^{n-j-1} (a_n x)^j$, it follows that $a_n \alpha$ is a root of a monic polynomial. The result is obtained by taking $d = a_n$. ■

• Comment. The above is simple enough that you should remember the argument rather than the theorem. This has the advantage that if you know a polynomial $f(x)$ that α is a root of, then you will know the value of d in the theorem.

Homework:

(1) Find a polynomial in $\mathbb{Z}[x]$ of degree 4 which has $1 + \sqrt{2} + \sqrt{3}$ as a root. Simplify your answer.

(2) Prove that $\dfrac{1}{\pi} \sin^{-1} \left(\dfrac{\sqrt[3]{2}}{3} \right)$ is irrational.

(3) Let α be non-zero. Prove that α and $1/\alpha$ are both algebraic integers if and only if α is a root of a monic polynomial in $\mathbb{Z}[x]$ and α is a root of a polynomial in $\mathbb{Z}[x]$ with constant term 1.

Minimal Polynomials:

• Definition. Let α be an algebraic number. Then the *minimal polynomial* for α (in $\mathbb{Q}[x]$) is the monic polynomial in $\mathbb{Q}[x]$ of minimal degree which has α as a root. (Note the first homework assignment below.)

• Goal for this section. We will establish:

Theorem 7. *The minimal polynomial for an algebraic number α is in $\mathbb{Z}[x]$ if and only if α is an algebraic integer.*

• A lemma of Gauss.

Definition. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$. Then the *content* of $f(x)$ is $\gcd(a_n, a_{n-1}, \dots, a_1, a_0)$. If the content of $f(x)$ is 1, then $f(x)$ is *primitive*.

Lemma. *If $u(x)$ and $v(x)$ are primitive polynomials, then so is $u(x)v(x)$.*

Proof. It suffices to prove that the content of $u(x)v(x)$ is not divisible by each prime. Let p be a prime. Write $u(x) = \sum_{j=0}^{n} a_j x^j$ and $v(x) = \sum_{j=0}^{m} b_j x^j$. Let k and ℓ be non-negative integers as small as possible such that $p \nmid a_k$ and $p \nmid b_\ell$; these exist since $u(x)$ and $v(x)$ are primitive. One checks that the coefficient of $x^{k+\ell}$ is not divisible by p. It follows that the content of $u(x)v(x)$ cannot be divisible by p, completing the proof. ■

Theorem 8 (Gauss' Lemma). *Let $f(x) \in \mathbb{Z}[x]$. Suppose that there exist $u_1(x)$ and $v_1(x)$ in $\mathbb{Q}[x]$ such that $f(x) = u_1(x)v_1(x)$. Then there exist $u_2(x)$ and $v_2(x)$ in $\mathbb{Z}[x]$ such that $f(x) = u_2(x)v_2(x)$ and $\deg u_2(x) = \deg u_1(x)$ and $\deg v_2(x) = \deg v_1(x)$.*

Comment: The theorem implies that if $f(x) \in \mathbb{Z}[x]$ has content 1, then a necessary and sufficient condition for $f(x)$ to be irreducible over the rationals is for it be irreducible over the integers. Also, we note that the proof will show more, namely that one can take $u_2(x)$ and $v_2(x)$ to be rational numbers times $u_1(x)$ and $v_1(x)$, respectively.

Proof. Let d denote the content of $f(x)$. Then there are positive rational integers a and b and primitive polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u(x) = \deg u_1(x)$ and $\deg v(x) = \deg v_1(x)$ satisfying $u_1(x)v_1(x) = (a/b)u(x)v(x)$. Then there is a primitive $g(x) \in \mathbb{Z}[x]$ for which $f(x) = dg(x)$ and $bdg(x) = bf(x) = au(x)v(x)$. By the lemma, $u(x)v(x)$ is primitive. It follows that the content of $au(x)v(x)$ is a. Since $g(x)$ is primitive, the content of $bdg(x)$ is bd. Hence, $a = bd$. We set $u_2(x) = du(x)$ and $v_2(x) = v(x)$. Then $f(x) = u_1(x)v_1(x) = du(x)v(x) = u_2(x)v_2(x)$, and we deduce the theorem. ■

• The proof of Theorem 7. It is clear that if the minimal polynomial for α is in $\mathbb{Z}[x]$, then α is an algebraic integer. Now, consider an algebraic integer α, and let $f(x) \in \mathbb{Z}[x]$ be monic with $f(\alpha) = 0$. Let $u_1(x)$ be the minimal polynomial for α. We want to prove that $u_1(x) \in \mathbb{Z}[x]$. By the division algorithm for polynomials in $\mathbb{Q}[x]$, there exist $v_1(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $f(x) = u_1(x)v_1(x) + r(x)$ and either $r(x) \equiv 0$ or $0 \le \deg r(x) < \deg u_1(x)$. Note that $r(\alpha) = f(\alpha) - u_1(\alpha)v_1(\alpha) = 0$. Since $u_1(x)$ is the monic polynomial of smallest degree having α as a root, it follows that $r(x) \equiv 0$ (otherwise, there would be a $k \in \mathbb{Z}$ for which $(1/k)r(x) \in \mathbb{Q}[x]$ is monic, is of smaller degree than $\deg u_1(x)$, and has α as a root). Thus, $f(x) = u_1(x)v_1(x)$ is a factorization of $f(x)$ in $\mathbb{Q}[x]$. By Gauss' Lemma and the comment after it, there exist $u_2(x)$ and $v_2(x)$ in $\mathbb{Z}[x]$ with $f(x) = u_2(x)v_2(x)$ and with $u_2(x) = mu_1(x)$ for some non-zero rational number m. By considering $f(x) = (-u_2(x))(-v_2(x))$ if necessary, we may suppose that the leading coefficient of $u_2(x)$ is positive. Since $f(x)$ is monic, we deduce that $u_2(x)$ is monic. Comparing leading coefficients in $u_2(x) = mu_1(x)$, we see that $m = 1$ so that $u_1(x) = u_2(x) \in \mathbb{Z}[x]$ as desired.

Algebraic Number Fields:

• The definition. If α is an algebraic number, then $\mathbb{Q}(\alpha)$ is defined to be the smallest field containing both α and the rationals.

• Some simple observations. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial for α. By considering each integer $j \ge 0$ successively and $\alpha^j f(\alpha) = 0$, one shows that α^{n+j} can be expressed as a polynomial in α with coefficients in $\mathbb{Q}$ and with degree $\le n-1$. It follows that $\mathbb{Q}(\alpha)$ is the set of all numbers of the form $g(\alpha)/h(\alpha)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $\deg g(x) \le n-1$, $\deg h(x) \le n-1$, and $h(\alpha) \ne 0$. By Theorem 4, every element of $\mathbb{Q}(\alpha)$ is an algebraic number. For this reason, we refer to $\mathbb{Q}(\alpha)$ as an *algebraic number field*.

• The ring of algebraic integers in $\mathbb{Q}(\alpha)$.

Theorem 9. *The algebraic integers contained in an algebraic number field $\mathbb{Q}(\alpha)$ form a ring.*

Proof. If α and β are in $\mathbb{Q}(\alpha)$, then so are $\alpha\beta$ and $\alpha - \beta$ since $\mathbb{Q}(\alpha)$ is a field. If also α and β are algebraic integers, then Theorem 5 implies $\alpha\beta$ and $\alpha - \beta$ are algebraic integers. The result follows. ■

Homework:

(1) Prove that for every algebraic number α, the minimal polynomial for α exists and is unique.

(2) Prove that the minimal polynomial $f(x)$ for an algebraic number α is irreducible over the rationals. In other words, prove that there do not exist $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$ of degree ≥ 1 satisfying $f(x) = g(x)h(x)$.

(3) With the notation in the section above, let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x)$ with $\alpha_1 = \alpha$. Show that $w = h(\alpha_2)h(\alpha_3)\cdots h(\alpha_n) \in \mathbb{Q}[\alpha]$ (i.e., w can be expressed as a polynomial in α with rational coefficients). Also, show that $w \neq 0$. By considering $(g(\alpha)w)/(h(\alpha)w)$, show that every element of $\mathbb{Q}(\alpha)$ can be written uniquely in the form $u(\alpha)$ where $u(x) \in \mathbb{Q}[x]$ and $\deg u(x) \leq n-1$. (There are other ways to establish this; we will in fact do this momentarily. The homework problem is to establish this result about $\mathbb{Q}(\alpha)$ by showing that one can "rationalize the denominator" of $g(\alpha)/h(\alpha)$.)

Quadratic Extensions:

• Definition. Let $m \in \mathbb{Z}$ with m not a square. Then $\mathbb{Q}(\sqrt{m})$ is a *quadratic extension* of the rationals. Note that the minimal polynomial for $\sqrt{m}$ is $x^2 - m$ (see the first homework exercises, problem (5)).

• The elements of $\mathbb{Q}(\sqrt{m})$. We have discussed this in more generality already. If $\beta \in \mathbb{Q}(\sqrt{m})$, then there are rational integers a, b, c, and d such that

$$\beta = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} \times \frac{c - d\sqrt{m}}{c - d\sqrt{m}} = \frac{(ac - bdm) + (bc - ad)\sqrt{m}}{c^2 - md^2}.$$

Observe that the denominator is non-zero since $\sqrt{m} \notin \mathbb{Q}$. The above corresponds to what took place in the last homework problem; we have shown that each element of $\mathbb{Q}(\sqrt{m})$ can be expressed as a linear polynomial in $\sqrt{m}$ with coefficients in $\mathbb{Q}$. Note that each element of $\mathbb{Q}(\sqrt{m})$ has a *unique* representation of the form $a + b\sqrt{m}$ with a and b rational.

• When does $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$? One way to show two algebraic number fields are the same field is to show that $\alpha_1 \in \mathbb{Q}(\alpha_2)$ (so that $\mathbb{Q}(\alpha_2)$ is a field containing α_1) and that $\alpha_2 \in \mathbb{Q}(\alpha_1)$ (so that $\mathbb{Q}(\alpha_1)$ is a field containing α_2). Explain why this is enough.

• When does $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m'})$? Given the above, equality holds if there are positive integers k and ℓ such that $k^2 m = \ell^2 m'$. It follows that all quadratic extensions are of the form $\mathbb{Q}(\sqrt{m})$ with m a squarefree integer and $m \neq 1$. Since m squarefree implies m is not a square, these are all quadratic extensions. Are these all different? Suppose $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m'})$ with m and m' squarefree. Then $\sqrt{m} \in \mathbb{Q}(\sqrt{m'})$ implies that $\sqrt{m'm} \in \mathbb{Q}$ (with a tiny bit of work). It follows that $m = m'$.

• What are the algebraic integers in $\mathbb{Q}(\sqrt{m})$? We suppose now that m is a squarefree integer with $m \neq 1$. Note that $m \not\equiv 0 \pmod 4$. The algebraic integers in $\mathbb{Q}(\alpha)$ in general form a ring. We show the following:

Theorem 10. *The ring of algebraic integers in $\mathbb{Q}(\sqrt{m})$ (where m is a squarefree integer with $m \neq 1$) is*

$$R = \mathbb{Z}[\sqrt{m}] \qquad \text{if } m \equiv 2 \text{ or } 3 \pmod 4$$

and is

$$R = \left\{ \frac{a + b\sqrt{m}}{2} : a \in \mathbb{Z}, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \qquad \text{if } m \equiv 1 \pmod 4.$$

Proof. Let R' be the ring of algebraic integers in $\mathbb{Q}(\sqrt{m})$, and let R be defined as in the displayed equations above. Let $\beta \in \mathbb{Q}(\sqrt{m})$. The above implies we may write $\beta = (a+b\sqrt{m})/d$ where a, b, and d are integers with $d > 0$ and $\gcd(a,b,d) = 1$. From $(d\beta - a)^2 = b^2 m$, we obtain that β is a root of the quadratic $f(x) = x^2 - (2a/d)x + (a^2 - b^2 m)/d^2$. We easily deduce that $R \subseteq R'$.

To show $R' \subseteq R$, we consider $\beta \in R'$ and show it must be in R. If β is rational, then Theorem 2 implies that $\beta \in \mathbb{Z}$ and, hence, $\beta \in R$. Suppose then that $\beta \notin \mathbb{Q}$. Since β is a root of the monic quadratic $f(x)$, we deduce that $f(x)$ is the minimal polynomial for β. By Theorem 7, we obtain $d|(2a)$ and $d^2|(a^2 - b^2 m)$. The condition $\gcd(a,b,d) = 1$ implies $\gcd(a,d) = 1$ (otherwise, $p|\gcd(a,d)$ and $d^2|(a^2 - b^2 m)$ implies $p|b$). Since $d > 0$ and $d|(2a)$, we obtain that d is either 1 or 2.

If $d = 1$, then $\beta \in R$ as desired. So suppose $d = 2$. Since $\gcd(a,b,d) = 1$, at least one of a and b is odd. Since $d^2|(a^2 - b^2 m)$, we obtain $a^2 \equiv b^2 m \pmod 4$. Now, $m \not\equiv 0 \pmod 4$ implies that a and b are both odd. Therefore, $a^2 \equiv b^2 \equiv 1 \pmod 4$. The congruence $a^2 \equiv b^2 m \pmod 4$ gives that $m \equiv 1 \pmod 4$. The theorem follows. ■

Good Rational Approximations and Units:

• Given a real number α, what does it mean to have a good rational approximation to it? As we know, it is possible to obtain an arbitrary good approximation to α by using rational numbers. In other words, given an $\varepsilon > 0$, we can find a rational number a/b (here, a and b denote integers with $b > 0$) such that $|\alpha - (a/b)| < \varepsilon$. So how much better can "good" be? A proof of this ε result is helpful. Of course, one can appeal to the fact that the rationals are dense on the real line, but we consider a different approach. Let $b > 1/(2\varepsilon)$ and divide the number line into disjoint intervals $I = (k/b, (k+1)/b]$ of length $1/b$. The number α will lie in one of them. Consider the endpoints of this interval, and let a/b be the endpoint which is nearest to α (either endpoint will do if α is the midpoint). Then $|\alpha - (a/b)| \leq 1/(2b) < \varepsilon$.

• Answering the question. We can view the a/b we constructed as a rational approximation of α, but it is possible to have better approximations in the following sense. The above choice for a/b satisfies $|\alpha - (a/b)| \le 1/(2b)$. Let's prove now that there are a/b satisfying $|\alpha - (a/b)| < 1/b^2$ (but we note here a difference: for *infinitely many* positive integers b, there is an a for which a/b is within $1/b^2$ of being α; for *every* positive integer b, there is an a for which a/b is within $1/(2b)$ of being α). We use the Dirichlet drawer principle as Dirichlet himself did. Fix a positive integer N. For each $b \in [0, N]$, consider $a = [b\alpha]$ so that $b\alpha - a \in [0, 1)$. Two of these $N + 1$ values must be within $1/N$ of each other. More precisely, there are integers b_1 and b_2 in $[0, N]$ with $(b_2\alpha - a_2) - (b_1\alpha - a_1) \in [0, 1/N)$ for some integers a_1 and a_2. By taking $b = |b_2 - b_1| \in [1, N]$, and $a = \pm(a_2 - a_1)$, we deduce

$$|b\alpha - a| < \frac{1}{N} \implies \left|\alpha - \frac{a}{b}\right| < \frac{1}{bN} \le \frac{1}{b^2}.$$

• Avoiding the question further. What exactly "good" means is questionable. We will see later that for every real number α, there are infinitely many positive integers b such that $|\alpha - (a/b)| < 1/(\sqrt{5}\, b^2)$ for some integer a. Furthermore, the number $\sqrt{5}$ is best possible. Perhaps then such a/b should be considered good rational approximations of α. Or maybe those are great rational approximations and we should view any rational number a/b within $1/b^2$ of α or something close to that as being a good rational approximation. I didn't really intend to define good because what's good in general tends to depend on the individual asking the question, and whatever I tell you is good you might not believe anyway.

• Units and an example. A unit in a ring R is an element of R that has a multiplicative inverse. Let's consider R to be the ring of algebraic integers in $\mathbb{Q}(\sqrt{2})$. By Theorem 10, $R = \mathbb{Z}[\sqrt{2}]$. Let $\beta \in R$, so there are integers a and b such that $\beta = a + b\sqrt{2}$. We suppose β is a unit in R. Then

$$\frac{1}{\beta} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Z}[\sqrt{2}].$$

Thus, $(a^2 - 2b^2)|a$ and $(a^2 - 2b^2)|b$ (use the uniqueness of the representation $x + y\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$ where x and y are rational). Let $d = \gcd(a, b)$. Then $d^2|(a^2 - 2b^2)$ implies that $d^2|a$ and $d^2|b$. But this means $d^2 \le d$. We deduce that $d = 1$. On the other hand, $a^2 - 2b^2$ is a common divisor of a and b. It follows that $a^2 - 2b^2 = \pm 1$. Remember this for later. If $\beta = a + b\sqrt{2}$ is a unit in R, then $a^2 - 2b^2 = \pm 1$. The converse is easily seen to be true as well. We consider now the case when a and b are positive (the other solutions of $a^2 - 2b^2 = \pm 1$ can be obtained from these).

We obtain that

$$\left(\frac{a}{b} - \sqrt{2}\right)\left(\frac{a}{b} + \sqrt{2}\right) = \pm\frac{1}{b^2}$$

so that

$$\left|\sqrt{2} - \frac{a}{b}\right| = \frac{1}{\left(\frac{a}{b} + \sqrt{2}\right) b^2} < \frac{1}{\sqrt{2}\, b^2}.$$

We see then that a/b is in some sense a good rational approximation of $\sqrt{2}$. It is actually better than indicated here. To see this note that the above implies

$$\frac{a}{b} \geq \sqrt{2} - \frac{1}{\sqrt{2}\,b^2} \geq \sqrt{2} - \frac{1}{\sqrt{2}},$$

and we get

$$\left|\sqrt{2} - \frac{a}{b}\right| = \frac{1}{\left(\dfrac{a}{b} + \sqrt{2}\right)b^2} \leq \frac{1}{\left(2\sqrt{2} - \dfrac{1}{\sqrt{2}}\right)b^2} = \frac{1}{2.12132\cdots \times b^2} < \frac{1}{2\,b^2}.$$

We can repeat the above to show that a/b is still better than this suggests. One more time around, in fact, gives that $|\sqrt{2} - (a/b)| < 1/(\sqrt{5}\,b^2)$, a good approximation indeed.

• The units in $\mathbb{Z}[\sqrt{2}]$. We now show how one can determine the complete set of units in $\mathbb{Z}[\sqrt{2}]$. We begin with a lemma that basically asserts that the units in any ring form a mulitplicative group.

Lemma. *Let ϵ_1 and ϵ_2 be units in a ring R. Then $\epsilon_1\epsilon_2$ and $\epsilon_1\epsilon_2^{-1}$ are also units in R.*

Proof. Use that $\epsilon_1\epsilon_2$ and $\epsilon_2^{-1}\epsilon_1^{-1}$ are in R and their product is 1, and $\epsilon_1\epsilon_2^{-1}$ and $\epsilon_2\epsilon_1^{-1}$ are in R and their product is 1. ■

Comment: Let $u = 1 + \sqrt{2}$. Since $u(-1 + \sqrt{2}) = 1$, u is a unit in $R = \mathbb{Z}[\sqrt{2}]$. Clearly, -1 is a unit in R as well. By the lemma, $\pm u^n$ is a unit in R for every $n \in \mathbb{Z}$. In fact, we show the following:

Theorem 11. *The units in $\mathbb{Z}[\sqrt{2}]$ are precisely the numbers of the form $\pm(1+\sqrt{2})^n$ where $n \in \mathbb{Z}$.*

Proof. By the comment, it suffices to show that $\mathbb{Z}[\sqrt{2}]$ contains no more units than those indicated by the Theorem. Let $u = 1 + \sqrt{2}$. We first show that u is the only unit in $(1, u]$. Let $\epsilon = a + b\sqrt{2}$ be a unit in $(1, u]$ where a and b are in $\mathbb{Z}$. As seen before, we have $a^2 - 2b^2 = \pm 1$. From $a + b\sqrt{2} > 1$ and $1 = |a^2 - 2b^2| = |a - b\sqrt{2}||a + b\sqrt{2}|$, we deduce $-1 < a - b\sqrt{2} < 1$. Since $1 < a + b\sqrt{2} \leq 1 + \sqrt{2}$, we obtain $0 < 2a \leq 2 + \sqrt{2}$. Hence, $a = 1$. Now, $1 < 1 + b\sqrt{2} \leq 1 + \sqrt{2}$ implies $b = 1$, so $\epsilon = u$.

Now, suppose ϵ is an arbitrary unit in $\mathbb{Z}[\sqrt{2}]$. Clearly $\epsilon \in \mathbb{R}$. Note that ϵ is a unit if and only if $-\epsilon$ is, so we may restrict our attention to $\epsilon > 0$ and do so. Let $n \in \mathbb{Z}$ with $\epsilon \in (u^{n-1}, u^n]$. By the lemma, $\epsilon u^{-(n-1)}$ is a unit. Also, $\epsilon u^{-(n-1)}$ is in $(1, u]$. Hence, by the above, $\epsilon u^{-(n-1)} = u$ so that $\epsilon = u^n$, completing the proof. ■

• A corollary. As a consequence of the above discussion, we have the

Corollary. *The solutions of $x^2 - 2y^2 = \pm 1$ in integers x and y are determined by the equation $x + y\sqrt{2} = \pm(1 + \sqrt{2})^n$ where $n \in \mathbb{Z}$.*

Homework:

(1) Let $u = (1 + \sqrt{5})/2$. Prove that the units in the ring of algebraic integers in $\mathbb{Q}(\sqrt{5})$ are precisely those numbers of the form $\pm u^n$ where $n \in \mathbb{Z}$.

Simple Continued Fractions and Approximations:

- Definitions. The expression

$$(*) \qquad q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}}},$$

also written $[q_0, q_1, q_2, q_3, \dots]$, is called a continued fraction. We take the q_j, called partial quotients, to be real with $q_j > 0$ if $j > 0$. The numbers $c_0 = q_0, c_1 = [q_0, q_1], c_2 = [q_0, q_1, q_2], \dots$ are called the convergents of the continued fraction. The number of partial quotients in $(*)$ may be finite or infinite. In the case that the number is finite, the meaning of the value of the continued fraction is clear. In the case that there are infinitely many partial quotients, the value of the continued fraction is $\lim_{n\to\infty} c_n$ provided the limit exists.

- An easy way to calculate convergents.

Theorem 12. *Let $a_{-2} = 0$, $a_{-1} = 1$, $b_{-2} = 1$, and $b_{-1} = 0$. Define*

$$a_j = a_{j-1}q_j + a_{j-2} \quad \text{and} \quad b_j = b_{j-1}q_j + b_{j-2} \quad \text{for } j \in \{0, 1, 2, \dots\},$$

where the q_j are the partial quotients as in $(*)$. Then

$$c_j = \frac{a_j}{b_j} \quad \text{for } j \in \{0, 1, 2, \dots\}$$

and, furthermore,

$$a_j b_{j-1} - a_{j-1} b_j = (-1)^{j+1} \quad \text{for } j \in \{-1, 0, 1, 2, \dots\}.$$

Examples and Comments: Compute the values of $[1, 2, 4, 2]$, $[1, 2, 1, 3]$, and $[2, 3, 1, 1, 2]$ using Theorem 12. Note that one computes these values by beginning with q_0.

Proof of Theorem 12. We prove both parts by induction. One checks that $c_0 = q_0 = a_0/b_0$. Suppose k is a non-negative integer such that for all real numbers q_0 and all positive real numbers $q_1, \dots, q_k$, we have $a_k/b_k = [q_0, q_1, \dots, q_k]$ where a_k and b_k are as defined in the theorem. Now, fix a real number q_0 and positive real numbers $q_1, \dots, q_k, q_{k+1}$, and consider a_j and b_j as in the theorem. Define

$$a' = \left(q_k + \frac{1}{q_{k+1}}\right)a_{k-1} + a_{k-2} \quad \text{and} \quad b' = \left(q_k + \frac{1}{q_{k+1}}\right)b_{k-1} + b_{k-2}.$$

Observe that $[q_0, q_1, \ldots, q_k, q_{k+1}] = [q_0, q_1, \ldots, q_{k-1}, q_k + (1/q_{k+1})]$, and the induction hypothesis applies to the latter. Hence, the latter is a'/b'. On the other hand,

$$a_{k+1} = a_k q_{k+1} + a_{k-1} = (a_{k-1} q_k + a_{k-2}) q_{k+1} + a_{k-1}$$

and the analogous result for b_{k+1} imply that $a' = a_{k+1}/q_{k+1}$ and $b' = b_{k+1}/q_{k+1}$. Hence, $a_{k+1}/b_{k+1} = a'/b' = [q_0, q_1, \ldots, q_k, q_{k+1}]$.

One checks directly that the last equation in the theorem holds for $j = -1$. Suppose it holds for some $j = k \geq -1$. Then

$$\begin{aligned} a_{k+1} b_k - a_k b_{k+1} &= (a_k q_{k+1} + a_{k-1}) b_k - a_k (b_k q_{k+1} + b_{k-1}) \\ &= -(a_k b_{k-1} - a_{k-1} b_k) = (-1)^{k+2}, \end{aligned}$$

from which the result follows. ■

- Simple Continued Fractions. If q_0 is an integer and $q_1, q_2, \ldots$ are positive integers, then the continued fraction $[q_0, q_1, \ldots]$ is called a simple continued fraction. Throughout this section, we make use of the notation made in Theorem 12. Our main goal here is to show that simple continued fractions with infinitely many partial quotients converge (see Theorem 18). In each of the results stated below, we clarify however if the statments hold for continued fractions in general or if the statments hold specifically for simple continued fractions.

Theorem 13. *For simple continued fractions, the numbers a_j and b_j are relatively prime integers.*

Proof. This follows from $a_j b_{j-1} - a_{j-1} b_j = (-1)^{j+1}$ for $j \geq -1$. ■

Theorem 14. *For simple continued fractions, the numbers b_j satisfy $b_j \geq j$ for all $j \geq 0$.*

Proof. One checks directly that $b_j \geq j$ for $j = 0$ and $j = 1$. In fact, $b_0 = 1$. For $j > 1$, the result follows by induction since $b_j = b_{j-1} q_j + b_{j-2} \geq b_{j-1} + 1$. ■

Theorem 15. *For continued fractions, we have*

$$\frac{a_n}{b_n} - \frac{a_{n-1}}{b_{n-1}} = \frac{(-1)^{n+1}}{b_n b_{n-1}} \qquad \text{for all } n \geq 1$$

and

$$\frac{a_n}{b_n} - \frac{a_{n-2}}{b_{n-2}} = \frac{(-1)^n q_n}{b_n b_{n-2}} \qquad \text{for all } n \geq 2$$

Proof. The first of these follows immediately from $a_n b_{n-1} - a_{n-1} b_n = (-1)^{n+1}$ (see Theorem 12). Also, by definition, $b_n - b_{n-2} = q_n b_{n-1}$. Thus,

$$\begin{aligned} \frac{a_n}{b_n} - \frac{a_{n-2}}{b_{n-2}} &= \left(\frac{a_n}{b_n} - \frac{a_{n-1}}{b_{n-1}} \right) + \left(\frac{a_{n-1}}{b_{n-1}} - \frac{a_{n-2}}{b_{n-2}} \right) = \frac{(-1)^{n+1}}{b_n b_{n-1}} + \frac{(-1)^n}{b_{n-1} b_{n-2}} \\ &= \frac{(-1)^n}{b_{n-1}} \left(\frac{b_n - b_{n-2}}{b_n b_{n-2}} \right) = \frac{(-1)^n q_n b_{n-1}}{b_n b_{n-1} b_{n-2}} = \frac{(-1)^n q_n}{b_n b_{n-2}}. \end{aligned}$$ ■

Theorem 16. *For continued fractions, the convergents c_{2n} strictly increase for $n \geq 0$ and the convergents c_{2n+1} strictly decrease for $n \geq 0$.*

Proof. This follows immediately from the second equation in Theorem 15. ■

Theorem 17. *For continued fractions, if n and m are ≥ 0, then $c_{2m+1} > c_{2n}$.*

Proof. The first equation in Theorem 15 implies that $c_{2n-1} > c_{2n}$ if $n \geq 1$ and that $c_{2m+1} > c_{2m}$. If $m \leq n-1$ (so $n \geq 1$), then we use Theorem 16 to obtain $c_{2m+1} \geq c_{2n-1} > c_{2n}$. If $m \geq n$, then we use Theorem 16 to obtain $c_{2m+1} > c_{2m} \geq c_{2n}$. ■

Theorem 18. *For simple continued fractions containing infinitely many partial quotients, $\lim_{n\to\infty} c_n$ exists.*

Proof. By Theorems 16 and 17, the convergents c_{2n} are increasing and bounded above by c_1. Hence, $\lim_{n\to\infty} c_{2n}$ exists. Call this limit L. Consider an arbitrary $\varepsilon > 0$. Let N be a positive integer such that if $k \geq N$, then $|c_{2k} - L| < \varepsilon/2$ and $2k(2k+1) > 2/\varepsilon$. If n is an integer $\geq 2N$, then either $n = 2k$ with $k \geq N$ and $|c_n - L| < \varepsilon/2 < \varepsilon$ or $n = 2k+1$ with $k \geq N$ and (using Theorems 15 and 14)

$$|c_n - L| \leq |c_{2k+1} - c_{2k}| + |c_{2k} - L| < \frac{1}{b_{2k}b_{2k+1}} + \frac{\varepsilon}{2} \leq \frac{1}{2k(2k+1)} + \frac{\varepsilon}{2} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

The result follows. (Alternatively, one can use that $\lim_{n\to\infty} c_{2n}$ and $\lim_{n\to\infty} c_{2n+1}$ both exist and that $\lim_{n\to\infty} (c_{2n+1} - c_{2n}) = 0$.) ■

Comment: It is apparent that the convergents c_{2n} increase to $L = \lim_{n\to\infty} c_n$ and that the convergents c_{2n+1} decrease to L.

• Is every real number α the value of a simple continued fraction? The answer is, "Yes," and in fact every real number that is not rational has a unique representation as a simple continued fraction. We establish this next as well as a clarification of what happens in the case that $\alpha \in \mathbb{Q}$. By Theorem 18, we know that every simple continued fraction $[q_0, q_1, \ldots]$ has some unique value α. We will write $\alpha = [q_0, q_1, \ldots]$. In what follows, q_j denotes an integer with $q_j > 0$ for $j > 0$; however, q'_j will denote real numbers (which are possibly not integral) with $q'_j > 0$ if $j > 0$.

Lemma 1. *Suppose $\alpha = [q_0, q_1, \ldots]$. If $\alpha \notin \mathbb{Q}$, then $q_0 = [\alpha]$. If $\alpha \in \mathbb{Q}$, then either $q_0 = [\alpha]$ or $\alpha = [q_0, 1]$ (with no further partial quotients existing).*

Proof. The situation is clear if only one partial quotient exists. Suppose there are more. We have already seen that $c_{2n} \leq \alpha \leq c_{2n+1}$ for all n so that, in particular, $q_0 \leq \alpha \leq [q_0, q_1]$. Since $q_1 \geq 1$, we have $q_0 \leq \alpha \leq q_0 + 1$ with $\alpha = q_0 + 1$ only in the case that $q_1 = 1$ and no further partial quotients exist. The result follows. ■

Lemma 2. *Define a_j and b_j for $j \in \{-2, -1, 0, \ldots, n-1\}$ as in Theorem 12 with the partial quotients $q_0, q_1, \ldots, q_{n-1}$. Then*

$$\alpha = [q_0, q_1, \ldots, q_{n-1}, q'_n] \quad \Longleftrightarrow \quad q'_n = \frac{a_{n-2} - b_{n-2}\alpha}{b_{n-1}\alpha - a_{n-1}}.$$

Proof. A simple manipulation gives

$$\alpha = \frac{a_{n-1}q_n' + a_{n-2}}{b_{n-1}q_n' + b_{n-2}} \qquad \Longleftrightarrow \qquad q_n' = \frac{a_{n-2} - b_{n-2}\alpha}{b_{n-1}\alpha - a_{n-1}}$$

(upon noting that if α is as on the left-hand side, the denominator on the right-hand side cannot be 0 because of the last equation in Theorem 12). Theorem 12 implies

$$[q_0, q_1, \ldots, q_{n-1}, q_n'] = \frac{a_{n-1}q_n' + a_{n-2}}{b_{n-1}q_n' + b_{n-2}},$$

and the result follows. ■

Lemma 3. *Suppose* $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n']$. *Then*

$$\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n, q_{n+1}, \ldots] \qquad \Longleftrightarrow \qquad q_n' = [q_n, q_{n+1}, \ldots].$$

Proof. As before, we let c_j denote the convergents of $[q_0, q_1, \ldots, q_{n-1}, q_n, q_{n+1}, \ldots]$. We let d_j denote the convergents of $[q_n, q_{n+1}, \ldots]$ so that $d_0 = q_n, d_1 = [q_n, q_{n+1}], \ldots$. Then $c_{n+k} = [q_0, q_1, \ldots, q_{n-1}, d_k]$. If $q_n' = [q_n, q_{n+1}, \ldots]$, then $\lim_{k\to\infty} d_k = q_n'$ so that $\lim_{n\to\infty} c_n = \lim_{k\to\infty} c_{n+k} = [q_0, q_1, \ldots, q_{n-1}, q_n'] = \alpha$. This implies $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n, q_{n+1}, \ldots]$. On the other hand, if we know $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n, q_{n+1}, \ldots]$, then $\alpha = \lim_{k\to\infty} c_{n+k} = \lim_{k\to\infty} [q_0, q_1, \ldots, q_{n-1}, d_k] = [q_0, q_1, \ldots, q_{n-1}, L]$ for some L by Theorem 18. Lemma 2 now implies that $L = q_n'$. Thus, $\lim_{k\to\infty} d_k = q_n'$, and we obtain $q_n' = [q_n, q_{n+1}, \ldots]$. ■

Suppose now that $\alpha \in \mathbb{R} - \mathbb{Q}$. We consider $q_0 = [\alpha]$ and $q_1' = 1/(\alpha - q_0)$ so that $\alpha = [q_0, q_1']$. Note that $\alpha - q_0 = \alpha - [\alpha] \in (0, 1)$ so that $q_1' > 1$. This choice for q_0 is motivated by Lemma 1. Also, motivated by Lemma 3 and Lemma 1, we consider $q_1 = [q_1'] \geq 1$ and $q_2' = 1/(q_1' - q_1) > 1$. Thus, $\alpha = [q_0, q_1, q_2']$. Continuing in this manner, we obtain $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n']$ where $q_n' = 1/(q_{n-1}' - q_{n-1}) > 1$. By Theorem 18, we know that $[q_0, q_1, q_2, \ldots] = L$ for some L. We prove next that $L = \alpha$. Let c_j denote the convergents of $[q_0, q_1, q_2, \ldots]$. By considering $\alpha = [q_0, q_1, \ldots, q_{2n}, q_{2n+1}, q_{2n+2}']$ in Theorem 16, we deduce that $c_{2n} \leq \alpha$ for every $n \geq 1$. By considering $\alpha = [q_0, q_1, \ldots, q_{2n+1}, q_{2n+2}, q_{2n+3}']$ in Theorem 16, we deduce that $c_{2n+1} \geq \alpha$ for every $n \geq 1$. By the Squeeze Theorem for limits, we obtain $L = \alpha$. Thus, α is the value of some simple continued fraction.

Is this value unique? Suppose $\alpha = [q_0, q_1, \ldots]$. Then by Lemma 1, q_0 is uniquely determined. Also, Lemma 2 or Lemma 3 implies that the q_1' we determined above with $\alpha = [q_0, q_1']$ is uniquely determined. By Lemma 3, $q_1' = [q_1, q_2, \ldots]$. Now, we are back where we started. Lemma 1 implies q_1 is uniquely determined, and Lemma 2 and Lemma 3 imply q_2' is uniquely determined with $q_1' = [q_1, q_2']$ and $q_2' = [q_2, q_3, \ldots]$. Continuing, we deduce that α has a unique representation as a simple continued fraction $[q_0, q_1, \ldots]$.

What if $\alpha \in \mathbb{Q}$? We proceed as above. First, if $\alpha = m \in \mathbb{Z}$, then $\alpha = [m]$ and also $\alpha = [m-1, 1]$. Otherwise, we consider $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n']$ with $q_n' > 1$ as we did before. Since $\alpha \in \mathbb{Q}$, so is q_n'. If $q_n' = m \in \mathbb{Z}$, then $\alpha = [q_0, q_1, \ldots, q_{n-1}, m] =$

$[q_0, q_1, \dots, q_{n-1}, m-1, 1]$. Otherwise, write $q'_n = a/b$ with a and b relatively prime positive integers and $a > b$. By the division algorithm, there exist a positive integer q_n and a remainder $r \in (0, b)$ such that $a = bq_n + r$. We get $a/b = [q_n, q'_{n+1}]$ with $q'_{n+1} = b/r > 1$. We continue as before with the one difference that we stop when some q'_n is an integer. Note also, however, that we just showed that if $q'_n = a/b \notin \mathbb{Z}$, then q'_{n+1} can be expressed as a rational number with a positive denominator strictly less than b. This implies that eventually, for some n, we will have $q'_n \in \mathbb{Z}$. As we have just seen, this will give us two representations of α as a simple continued fraction. The argument that these representations are the only such representations follows like the uniqueness argument in the case that $\alpha \notin \mathbb{Q}$ (the difference being in the use of Lemma 1). Summarizing, we have the following two theorems:

Theorem 19. *If $\alpha \in \mathbb{R} - \mathbb{Q}$, then α has a unique representation as a simple continued fraction.*

Theorem 20. *The simple continued fraction representation for $\alpha \in \mathbb{R}$ is finite if and only if $\alpha \in \mathbb{Q}$. If $\alpha \in \mathbb{Q}$, then there are unique integers $q_0, q_1, \dots, q_n$ with $q_j > 0$ for $j > 0$ such that $\alpha = [q_0, q_1, \dots, q_n] = [q_0, q_1, \dots, q_n - 1, 1]$. In particular, we may arrange for the simple continued fraction representation for $\alpha \in \mathbb{Q}$ to have an even or an odd number of partial quotients (whichever we choose).*

Comments and Examples: The numbers q'_n above are called the complete quotients for the simple continued fraction $\alpha = [q_0, q_1, \dots]$. It is also appropriate here to consider $q'_0 = \alpha$. As examples of the above material, derive the simple continued fraction representations for $10/7$ and $\sqrt{2}$.

Homework:

(1) Compute the simple continued fraction representation for $\sqrt{3}$.

(2) Compute the simple continued fraction representation for $\sqrt{n^2+1}$ where n is a positive integer.

(3) Let α be the positive real root of $x^3 - x - 1$. There is only one such root by Descartes' Rule of Signs. Calculate the first 3 partial quotients q_0, q_1, and q_2 of the simple continued fraction representation for α as follows (yes, you must do it this way to get credit). First, calculate q_0 by using the Intermediate Value Theorem. Then find a polynomial with q'_1 as a root. Then calculate q_1 by using the Intermediate Value Theorem and find a polynomial with q'_2 as a root. Finally, use the Intermediate Value Theorem to obtain q_2. Show your work.

• Good approximations by simple continued fractions. Throughout this section a and b will denote integers. We will refer to "the" simple continued fraction for α somewhat inappropriately given the content of Theorem 20 (there are actually two simple continued fraction representations for α if $\alpha \in \mathbb{Q}$).

Theorem 21. *Let $\alpha \in \mathbb{R}$. If a/b is a convergent of the simple continued fraction for α*

with $\gcd(a,b)=1$*, then*

$$\left|\alpha - \frac{a}{b}\right| \le \frac{1}{b^2}.$$

Proof. Let $n \ge 0$ be such that $a_n = a$ and $b_n = b$. If $\alpha = a_n/b_n$, then the result is clear. Otherwise, there is a further convergent a_{n+1}/b_{n+1} of the simple continued fraction for α. Since a_{n+1}/b_{n+1} and a_n/b_n are on opposite sides of α on the number line, we obtain from Theorem 15 that

$$\left|\alpha - \frac{a}{b}\right| \le \left|\frac{a_{n+1}}{b_{n+1}} - \frac{a_n}{b_n}\right| \le \frac{1}{b_n b_{n+1}} \le \frac{1}{b_n^2} = \frac{1}{b^2},$$

completing the proof. ■

Theorem 22. *Let* $\alpha \in \mathbb{R}$*. For every two consecutive convergents of the simple continued fraction for* α*, one of the convergents, say* a/b *with* $\gcd(a,b)=1$*, satisfies*

$$\left|\alpha - \frac{a}{b}\right| \le \frac{1}{2b^2}.$$

Proof. Let a_n/b_n and a_{n+1}/b_{n+1} be two consecutive convergents of the simple continued fraction for α. Assume that

$$\left|\alpha - \frac{a_n}{b_n}\right| > \frac{1}{2b_n^2} \quad \text{and} \quad \left|\alpha - \frac{a_{n+1}}{b_{n+1}}\right| > \frac{1}{2b_{n+1}^2}.$$

Since α is between a_n/b_n and a_{n+1}/b_{n+1}, we get from Theorem 15 that

$$\frac{1}{b_n b_{n+1}} = \left|\frac{a_{n+1}}{b_{n+1}} - \frac{a_n}{b_n}\right| = \left|\frac{a_{n+1}}{b_{n+1}} - \alpha\right| + \left|\alpha - \frac{a_n}{b_n}\right| > \frac{1}{2b_{n+1}^2} + \frac{1}{2b_n^2}.$$

It follows that $2b_{n+1}b_n > b_n^2 + b_{n+1}^2$ so that $(b_n - b_{n+1})^2 < 0$, a contradiction. The theorem follows. ■

Theorem 23. *Let* $\alpha \in \mathbb{R}$*. Suppose that*

$$\left|\alpha - \frac{a}{b}\right| \le \frac{1}{2b^2}.$$

Then a/b *is a convergent of the simpled continued fraction for* α*.*

Proof. We may suppose that $\gcd(a,b)=1$ and do so. Write $a/b = [q_0, q_1, \dots, q_n]$ where by Theorem 20 we can choose n to be either even or odd. We take n so that

$$\alpha - \frac{a}{b} = \frac{(-1)^n}{b^2}\theta \quad \text{with} \quad 0 \le \theta \le \frac{1}{2}.$$

Let a_k/b_k denote the convergents of $[q_0, q_1, \dots, q_n]$. Note that if $\alpha = a/b$, then $a/b = a_n/b_n$ and we're done. Suppose now that $\alpha \ne a/b$. Define $\beta \in \mathbb{R}$ so that

$$\alpha = \frac{\beta a_n + a_{n-1}}{\beta b_n + b_{n-1}}.$$

Using Theorem 12, we obtain

$$\begin{aligned}\frac{(-1)^{n+1}\theta}{b_n^2} &= \frac{a_n}{b_n} - \alpha = \frac{a_n(\beta b_n + b_{n-1}) - b_n(\beta a_n + a_{n-1})}{b_n(\beta b_n + b_{n-1})} \\ &= \frac{a_n b_{n-1} - a_{n-1} b_n}{b_n(\beta b_n + b_{n-1})} = \frac{(-1)^{n+1}}{b_n(\beta b_n + b_{n-1})}.\end{aligned}$$

It follows that $(\theta/b_n)(\beta b_n + b_{n-1}) = 1$. We deduce that

$$\beta = \frac{1}{\theta} - \frac{b_{n-1}}{b_n} \geq 2 - 1 = 1$$

since $\theta \leq 1/2$ and $b_n = b_{n-1}q_n + b_{n-2} \geq b_{n-1}$ (by considering whether $n = 0$ or $n > 0$ separately). Thus, there are positive integers $q_{n+1}, q_{n+2}, \dots$ such that $\beta = [q_{n+1}, q_{n+2}, \dots]$. Since $\alpha = (\beta a_n + a_{n-1})/(\beta b_n + b_{n-1})$ is the last convergent of $[q_0, q_1, \dots, q_n, \beta]$ (by Theorem 12), we get $\alpha = [q_0, q_1, \dots, q_n, \beta]$. From Lemma 3, we obtain $\alpha = [q_0, q_1, \dots, q_n, q_{n+1}, \dots]$. Thus, $a/b = a_n/b_n$ is a convergent of the simple continued fraction for α, completing the proof. ■

Corollary. *If a and b are positive integers and $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, then a/b is a convergent of the simple continued fraction for $\sqrt{2}$.*

Proof. We saw previously that if a and b are positive integers and $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, then

$$\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{2b^2}$$

so that the result follows immediately from Theorem 23. ■

Homework:

(1) Prove that Theorem 22 holds with strict inequality unless $\alpha = [m, 1, 1] = m + (1/2)$ for some integer m and the two consecutive convergents are m and $m + 1$. (Hint: In the proof of Theorem 14, it is almost the case that the b_j's are strictly increasing.)

(2) Let $\varepsilon > 1/2$. Prove that in Theorem 23 the expression $1/(2b^2)$ cannot be replaced by ε/b^2. (Hint: You might want to consider $\alpha = [0, m, 2, m] = [0, m, 2, m-1, 1]$ where m is a large positive integer. Note that $1/(m+1)$ will be a fairly good rational approximation of α but it is not a convergent of $[0, m, 2, m]$ or $[0, m, 2, m-1, 1]$.)

(3) Let $[x]$ denote the greatest integer $\leq x$. Determine whether the inequality

$$(*) \qquad \left[\frac{\pi}{2} b\right] < \frac{\pi}{2} b^2 \sin(1/b) \leq \frac{\pi}{2} b$$

holds for every positive integer b. If it does, supply a proof. If it doesn't, determine the least six postive integers b for which $(*)$ does not hold.

• Units in quadratic extensions. We are now ready to use simple continued fractions to obtain the units in real quadratic extensions.

Theorem 24. *Let m be a squarefree integer > 1, and let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{m})$. Suppose $x + y\sqrt{m} \in R$. Then $x + y\sqrt{m}$ is a unit in R if and only if $x^2 - my^2 = \pm 1$.*

Proof. If $x^2 - my^2 = \pm 1$, then it is easy to check that $\pm(x - y\sqrt{m})$ is in R and is the inverse of $x + y\sqrt{m}$. Hence, $x^2 - my^2 = \pm 1$ implies that $x + y\sqrt{m}$ is a unit in R. Now, suppose $x + y\sqrt{m}$ is a unit in R, and we want to show $x^2 - my^2 = \pm 1$. There exist rational numbers x' and y' such that $x' + y'\sqrt{m} \in R$ and

$$(*) \qquad 1 = (x + y\sqrt{m})(x' + y'\sqrt{m}) = (xx' + yy'm) + (xy' + x'y)\sqrt{m}.$$

We obtain $xx' + yy'm = 1$ and $xy' + x'y = 0$. Solving for x and y, we deduce

$$x = \frac{x'}{(x')^2 - m(y')^2} \qquad \text{and} \qquad y = \frac{-y'}{(x')^2 - m(y')^2}.$$

We obtain that $(x^2 - my^2)\big((x')^2 - m(y')^2\big) = 1$. Note that even if x and y are not integers, $x + y\sqrt{m} \in R$ implies that $x^2 - my^2 \in \mathbb{Z}$; similarly, $(x')^2 - m(y')^2 \in \mathbb{Z}$. Therefore, $(x^2 - my^2)\big((x')^2 - m(y')^2\big) = 1$ implies that $x^2 - my^2 = \pm 1$, completing the proof. ■

Examples: (1) Recall that $\sqrt{2} = [1, \overline{2}]$. The convergents are $1, 3/2, 7/5, 17/12, \dots$. The units $a + b\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ correspond to solutions of $a^2 - 2b^2 = \pm 1$. All the convergents a/b above satisfy this equation. In fact, if a and b are positive relatively prime integers with a/b a convergent of the simple continued fraction for $\sqrt{2}$, then $a^2 - 2b^2 = \pm 1$. More precisely, if a_n and b_n are as in Theorem 12 with $[q_0, q_1, \dots] = [1, \overline{2}]$, then $a_n^2 - 2b_n^2 = (-1)^{n+1}$. This follows easily by induction and the defining recursion relations for a_n and b_n. These comments should be considered with Theorem 11 and the Corollaries to Theorem 11 and Theorem 23.

(2) Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{13})$. By Theorem 24, the units $x + y\sqrt{13}$ in R are derived from solutions to $x^2 - 13y^2 = \pm 1$. We may suppose x and y are positive as other solutions come from replacing x with $\pm x$ and y with $\pm y$. If $x^2 - 13y^2 = \pm 1$ with x and y positive, we obtain

$$\left|\sqrt{13} - \frac{x}{y}\right| = \frac{1}{\left|\sqrt{13} + \dfrac{x}{y}\right| y^2} \le \frac{1}{\sqrt{13}y^2} < \frac{1}{2y^2}.$$

This would imply by Theorem 23 that x/y is a convergent of the simple continued fraction for $\sqrt{13}$ except that we do not know that x and y are integral. If x and y are integers, then x/y will be a convergent. Since $13 \equiv 1 \pmod 4$, we might have $x = x'/2$ and $y = y'/2$ for some odd integers x' and y'. Note in this case x'/y' might not be a sufficiently good approximation to ensure from Theorem 23 that it is a convergent. On the other hand, even if Theorem 23 does not apply, x'/y' is a somewhat good approximation to $\sqrt{13}$ and it might happen that it is a convergent of the simple continued fraction for $\sqrt{13}$. How can we tell? Observe that $x^2-13y^2=\pm1$ with $x=x'/2$ and $y=y'/2$ implies $(x')^2-13(y')^2=\pm4$. A computation gives $\sqrt{13}=[3,\overline{1,1,1,1,6}]$ with convergents

$$\frac{3}{1},\ \frac{4}{1},\ \frac{7}{2},\ \frac{11}{3},\ \frac{18}{5},\ \frac{119}{33},\ \frac{137}{38},\dots.$$

One checks these convergents by considering $3^2-13\times1^2=-4$, $4^2-13\times1^2=3$, $7^2-13\times2^2=-3$, $11^2-13\times3^2=4$, $18^2-13\times5^2=-1$, $119^2-13\times33^2=4$, etc. This gives us the units

$$18+5\sqrt{13},\qquad \frac{3+\sqrt{13}}{2},\qquad \frac{11+3\sqrt{13}}{2},\qquad \text{and}\qquad \frac{119+33\sqrt{13}}{2}.$$

Past experience would lead us to consider the possibility that the smallest unit above, namely $u=(3+\sqrt{13})/2$, may generate all the units in R. In fact, it can be shown using methods before that the units in R are precisely the numbers of the form $\pm u^n$ where $n\in\mathbb{Z}$.

Comment: We could probably have obtained the unit $(3+\sqrt{13})/2$ by trial and error (without simple continued fractions); but if you doubt the usefulness of simple continued fractions for this purpose, try describing the units in $\mathbb{Z}[\sqrt{94}]$ using a trial and error approach. The units are the numbers of the form $\pm u^n$ where $n\in\mathbb{Z}$ and $u=2143295+221064\sqrt{94}$.

• Hurwitz Theorem and others. We will not need the material in this section for the remainder of the course, but it is worth discussing it now that we have gone thus far.

Theorem 25 (Hurwitz). *Let $\alpha\in\mathbb{R}-\mathbb{Q}$. Then there exist infinitely many distinct rational numbers a/b (with a and b integers) such that*

$$(*)\qquad \left|\alpha-\frac{a}{b}\right|<\frac{1}{\sqrt{5}b^2}.$$

Furthermore, if $c>\sqrt{5}$, then $(*)$ cannot be improved by replacing $\sqrt{5}$ with c.

Proof. We show that one of every three consecutive convergents a/b of the simple continued fraction for α satisfies $(*)$. Assume that $(*)$ does not hold with $(a,b)=(a_{n-1},b_{n-1})$ and with $(a,b)=(a_n,b_n)$ (where $n\ge1$). We show

$$(**)\qquad \frac{b_n}{b_{n-1}}+\frac{b_{n-1}}{b_n}<\sqrt{5}$$

(given the assumption). In fact, this follows since α is between a_{n-1}/b_{n-1} and a_n/b_n so that

$$\frac{1}{b_{n-1}b_n}=\left|\frac{a_n}{b_n}-\frac{a_{n-1}}{b_{n-1}}\right|=\left|\alpha-\frac{a_n}{b_n}\right|+\left|\alpha-\frac{a_{n-1}}{b_{n-1}}\right|\ge\frac{1}{\sqrt{5}b_n^2}+\frac{1}{\sqrt{5}b_{n-1}^2}.$$

This implies $(**)$ upon noting that equality cannot hold in $(**)$ given that one side of the inequality is rational and the other is irrational. Taking $x=b_n/b_{n-1}$ in $(**)$, we obtain $x+x^{-1}<\sqrt{5}$ and $x\ge1$. Hence,

$$\left(x-\frac{\sqrt{5}+1}{2}\right)\left(x-\frac{\sqrt{5}-1}{2}\right)=x^2-\sqrt{5}x+1<0,$$

and we deduce that $x < (\sqrt{5}+1)/2$ (since $x \geq 1 > (\sqrt{5}-1)/2$). Thus, we obtain $b_n/b_{n-1} < (\sqrt{5}+1)/2$. Now, if $(*)$ does not hold for $(a,b) = (a_{n+1}, b_{n+1})$ as well, then by replacing n with $n+1$ above, we obtain $b_{n+1}/b_n < (\sqrt{5}+1)/2$. Since $b_{n+1} = b_n q_{n+1} + b_{n-1}$, we deduce

$$1 \leq q_{n+1} = \frac{b_{n+1}}{b_n} - \frac{b_{n-1}}{b_n} < \frac{\sqrt{5}+1}{2} - \frac{2}{\sqrt{5}+1} = 1,$$

a contradiction. Thus, $(*)$ holds for one of a_{n-1}/b_{n-1}, a_n/b_n, and a_{n+1}/b_{n+1} for each $n \geq 1$.

Now, let $c > \sqrt{5}$, and assume a and b are integers with $b > 0$ and $|\alpha - (a/b)| < 1/(cb^2)$. Note that if $a' \neq a$, then

$$\left|\alpha - \frac{a'}{b}\right| \geq \left|\frac{a'}{b} - \frac{a}{b}\right| - \left|\alpha - \frac{a}{b}\right| \geq \frac{1}{b} - \frac{1}{2b^2} \geq \frac{1}{2b} \geq \frac{1}{2b^2} > \frac{1}{cb^2}.$$

Therefore, it suffices to show that for some real number α the inequality $|\alpha - (a/b)| < 1/(cb^2)$ implies b is bounded. We take $\alpha = (\sqrt{5}-1)/2$. Then $|\alpha - (a/b)| < 1/(cb^2)$ implies that $\alpha = (a/b) + (\varepsilon/cb^2)$ for some ε with $|\varepsilon| \leq 1$. Multiplying by b and rearranging, we deduce that

$$\frac{\varepsilon}{cb} - \frac{\sqrt{5}b}{2} = \frac{-b}{2} - a.$$

Squaring we obtain

$$\frac{\varepsilon^2}{c^2b^2} - \frac{\sqrt{5}\,\varepsilon}{c} = \frac{-5b^2}{4} + \frac{b^2}{4} + ab + a^2 = a^2 + ab - b^2.$$

Observe that $|\sqrt{5}\,\varepsilon/c| \leq \sqrt{5}/c < 1$ and $a^2+ab-b^2 \in \mathbb{Z}$. We deduce that if b is sufficiently large ($b > (c^2 - c\sqrt{5})^{-1/2}$ will do), then a^2+ab-b^2 is a rational integer which has absolute value < 1. Thus, $a^2+ab-b^2 = 0$. This implies $(2a+b)^2 - 5b^2 = 0$, which is a contradiction since $\sqrt{5} \notin \mathbb{Q}$. ■

Comment: The choice for α in the above argument can be motivated by revisiting the proof of Theorem 21. From that argument, we see that

$$\left|\alpha - \frac{a_n}{b_n}\right| \leq \frac{1}{b_n b_{n+1}} \qquad \text{where} \qquad b_{n+1} = q_{n+1}b_n + b_{n-1}.$$

It follows that a_n/b_n will approximate α rather well if the partial quotient q_{n+1} is large. It is reasonable then to consider α in the last proof to have small partial quotients. We chose $\alpha = (\sqrt{5}-1)/2$ which can be represented as the simple continued fraction $[0, \overline{1}]$. As it turns out, for a fixed irrational number α, the constant $\sqrt{5}$ in the inequality in Theorem 25 cannot be improved if and only if the simple continued fraction for α is of the form $[q_0, q_1, \ldots]$ where for some positive integer n we have $q_n = q_{n+1} = q_{n+2} = \cdots = 1$ (all the partial quotients from some point on are 1). If we consider other irrational numbers not of this form, then for each of these the number $\sqrt{5}$ in the inequality in Theorem 25 can be replaced by $2\sqrt{2}$. This process continues (we can remove a certain set of irrational numbers from consideration and replace $2\sqrt{2}$ by an even larger number).

The above discussion leads naturally to the question, "For a given fixed α, how well can we approximate it by rational numbers?" As it turns out, if α can be approximated too well by rationals, then it must be either rational or transcendental. Rational numbers have the property that they can be approximated very well (by themselves). On the other hand, an irrational number with sufficiently "good" rational approximations cannot be algebraic. This observation was first made by Liouville and led him to the first proof that transcendental numbers exist.

Theorem 26 (Liouville). *Let α be a root of $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $\alpha \notin \mathbb{Q}$ and $f(x)$ non-zero. Then there is a constant $A > 0$ (depending on α and $f(x)$) such that if a and b are integers with $b > 0$, then*

$$\left|\alpha - \frac{a}{b}\right| > \frac{A}{b^n}.$$

Proof. Let M be the maximum value of $|f'(x)|$ on $[\alpha - 1, \alpha + 1]$, and note that $M > 0$. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ denote the distinct roots of $f(x)$ different from α. Fix

$$A < \min\left\{\frac{1}{M}, 1, |\alpha - \alpha_1|, |\alpha - \alpha_2|, \ldots, |\alpha - \alpha_m|\right\}.$$

Assume for some integers a and b with $b > 0$ we have $|\alpha - (a/b)| \le A/b^n$. In particular, $|\alpha - (a/b)| \le A$ so that $a/b \in [\alpha - 1, \alpha + 1]$ and $a/b \notin \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$. Thus, $f(a/b) \ne 0$. By the Mean Value Theorem, there is an $x_0 \in (\alpha - 1, \alpha + 1)$ such that

$$f(\alpha) - f(a/b) = \left(\alpha - \frac{a}{b}\right) f'(x_0).$$

The left-hand side is non-zero; hence, $f'(x_0) \ne 0$. Also, $f(a/b) \ne 0$ implies

$$|f(a/b)| = \frac{|a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b^n|}{b^n} \ge \frac{1}{b^n}.$$

Since $|f'(x_0)| \le M$, we deduce that

$$\left|\alpha - \frac{a}{b}\right| = \frac{|f(\alpha) - f(a/b)|}{|f'(x_0)|} = \frac{|f(a/b)|}{|f'(x_0)|} \ge \frac{1}{Mb^n} > \frac{A}{b^n} \ge \left|\alpha - \frac{a}{b}\right|,$$

a contradiction. The theorem follows. ∎

Corollary (Liouville). *There exist transcendental numbers. In particular, $\displaystyle\sum_{j=0}^{\infty} 10^{-j!}$ is transcendental.*

Proof. Call the sum α. It is not rational as it has a non-terminating decimal expansion with arbitrarily long blocks of zeroes. We show that for all positive integers n, there exist integers a and b with $b \geq 2$ such that $|\alpha - (a/b)| < 1/b^n$. Theorem 26 will then imply α is transcendental (why ?). Write $\sum_{j=0}^{n} 10^{-j!} = a/b$ with $b = 10^{n!}$. Then

$$\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots\right) < \frac{2}{\left(10^{n!}\right)^{n+1}} \leq \frac{1}{b^n}.$$

The result follows. ■

Stronger results than Theorem 26 exist. In particular, the following is classical (we will not prove it here).

Theorem 27 (Thué-Siegel-Roth). *Let $\alpha \in \mathbb{R} - \mathbb{Q}$ with α algebraic. Let $\varepsilon > 0$. Then there are at most finitely many integer pairs (a, b) with $b > 0$ such that $|\alpha - (a/b)| < 1/b^{2+\varepsilon}$.*

The following are two related open problems. The problems are in fact equivalent.

Open Problem 1. Let $\alpha \in \mathbb{R} - \mathbb{Q}$ with α algebraic. Does there exist an $A = A(\alpha) > 0$ such that if (a, b) is an integer pair with $b > 0$, then $|\alpha - (a/b)| > A/b^2$.

Open Problem 2. Let $\alpha \in \mathbb{R} - \mathbb{Q}$ with α algebraic. Does there exist a $B = B(\alpha)$ such that if $\alpha = [q_0, q_1, \ldots]$, then $q_j \leq B$ for all $j \in \{0, 1, 2, \ldots\}$?

It is not known whether there exists an algebraic number with minimal polynomial of degree ≥ 3 which has bounded partial quotients. It is also not known whether there exists an algebraic number with minimal polynomial of degree ≥ 3 which has unbounded partial quotients.

Homework:

(1) For n a positive integer, define rational integers x_n and y_n by $(1+\sqrt{2})^n = x_n + y_n\sqrt{2}$. Prove that if n is even and $a = x_n$ and $b = y_n$, then

$$\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{2\sqrt{2}b^2}.$$

(Hint: Look back at what we have done with units in $\mathbb{Z}[\sqrt{2}]$. Also, justify that $a/b = c_m$ for some *odd* integer m, actually $m = n - 1$.)

(2) Adjusting the argument for Theorem 26, show that if $c > 2\sqrt{2}$, then there are at most finitely many integers a and b with $b > 0$ such that

$$\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{cb^2}.$$

(3) Using Theorem 27, prove that there are at most finitely many integer pairs (x, y) for which $x^3 - 2y^3 = 1$.

(4) (a) Define $q_0 = 0$, $q_1 = 1$, and $q_n = q_{n-1}^2 + q_{n-2}$ for $n \geq 2$. Hence, $q_2 = 1$, $q_3 = 2$, $q_4 = 5$, $q_5 = 27$, and so on. Let $\alpha = [q_0, q_1, \ldots] = [0, 1, 1, 2, 5, 27, \ldots]$. For $n \geq 0$, we define

as usual $a_n/b_n = [q_0, q_1, \ldots, q_n]$ with a_n and b_n positive integers satisfying $\gcd(a_n, b_n) = 1$. Prove that $b_n = q_{n+1}$ for every integer $n \geq 0$.

(b) Prove that the number $\alpha = [0, 1, 1, 2, 5, 27, \ldots]$ from part (a) is transcendental. (Hint: α is between a_{n-1}/b_{n-1} and a_n/b_n and these are mighty close. Use Theorem 27.)

Simple Continued Fractions for Quadratic Irrationals:

• Eventually periodic simple continued fractions are quadratic irrationals. To see this, suppose first that $\beta = [\overline{q_0, q_1, \ldots, q_n}]$ (so β is purely periodic). Then $\beta = [q_0, q_1, \ldots, q_n, \beta]$. Defining a_j and b_j as in Theorem 12, we deduce that

$$\beta = \frac{\beta a_n + a_{n-1}}{\beta b_n + b_{n-1}}.$$

Rearranging, we obtain that β is a root of the quadratic $f(x) = b_n x^2 + (b_{n-1} - a_n)\beta - a_{n-1} \in \mathbb{Z}[x]$. Since β is not rational (it's simple continued fraction representation is infinite), we deduce that β is a quadratic irrational.

Now, suppose

$$\alpha = [q_0, q_1, \ldots, q_m, \overline{q_{m+1}, \ldots, q_{m+r}}],$$

and define a_j and b_j as in Theorem 12 (for this simple continued fraction). Set $\beta = [\overline{q_{m+1}, \ldots, q_{m+r}}]$. By the above, there are integers k, d, and ℓ with d not a square and $\ell \neq 0$ such that $\beta = (k + \sqrt{d})/\ell$ (if β is a root of $ax^2 + bx + c \in \mathbb{Z}[x]$, then either $\beta = (-b + \sqrt{b^2 - 4ac})/(2a)$ or $\beta = (b + \sqrt{b^2 - 4ac})/(-2a)$). Thus,

$$\alpha = \frac{\beta a_m + a_{m-1}}{\beta b_m + b_{m-1}} = \frac{u + v\sqrt{d}}{w}$$

for some integers u, v, and w with $w \neq 0$. It follows that α is a quadratic irrational (note that v cannot be 0 since the simple continued fraction expansion for α is infinite).

• A necessary and sufficient condition for being eventually periodic.

Lemma. *Let α be an algebraic number and $f(x) \in \mathbb{Q}[x]$ its minimal polynomial. Let $g(x) \in \mathbb{Q}[x]$ be such that $g(\alpha) = 0$. If β is such that $f(\beta) = 0$, then $g(\beta) = 0$. Moreover, $g(x)$ is divisible by $f(x)$ in $\mathbb{Q}[x]$.*

Proof. The lemma follows by considering $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $g(x) = f(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Since $f(x)$ is the minimal polynomial of α, one easily deduces that $r(x) = 0$, and the lemma follows. ∎

Theorem 28. *Let $\alpha \in \mathbb{R}$. Then the simple continued fraction for α is eventually periodic if and only if α is a quadratic irrational.*

Proof. Let α be a quadratic irrational. By the above, it suffices to show that the simple continued fraction for α is eventually periodic (the other implication in the theorem has already been established). Write

$$\alpha = \frac{k + \sqrt{d}}{\ell} = \frac{A_0 + \sqrt{N}}{B_0},$$

where $B_0 = \ell|\ell|$, $A_0 = k|\ell|$, and $N = d\ell^2$. Note that A_0, B_0, and N are integers satisfying $B_0|(N - A_0^2)$, $B_0 \neq 0$, and $N > 0$ is not a square. Define recursively

$$(*) \qquad w_j' = \frac{A_j + \sqrt{N}}{B_j}, \quad w_j = [w_j'], \quad A_{j+1} = w_j B_j - A_j, \quad \text{and} \quad B_{j+1} = \frac{N - A_{j+1}^2}{B_j},$$

where $j \in \{0, 1, 2, \dots\}$. We show first by induction that A_j and B_j are in $\mathbb{Z}$ with $B_j \neq 0$ and $B_j|(N - A_j^2)$. For $j = 0$, this has already been established. Suppose it is true for $j \leq m$. Since $w_m \in \mathbb{Z}$, we obtain $A_{m+1} = w_m B_m - A_m \in \mathbb{Z}$. It now follows that

$$B_{m+1} = \frac{N - (w_m B_m - A_m)^2}{B_m} = \frac{N - A_m^2}{B_m} - w_m^2 B_m + 2A_m w_m \in \mathbb{Z}.$$

Also, $B_m B_{m+1} = N - A_{m+1}^2$ so that $B_{m+1}|(N - A_{m+1}^2)$. Finally, $B_{m+1} = (N - A_{m+1}^2)/B_m$ is non-zero since $\sqrt{N}$ is irrational.

Observe that $w_0' = \alpha$ and, for $j \geq 0$,

$$\begin{aligned}
\frac{1}{w_j' - w_j} &= \frac{B_j}{(A_j - B_j w_j) + \sqrt{N}} = \frac{B_j(\sqrt{N} - (A_j - B_j w_j))}{N - (A_j - B_j w_j)^2} \\
&= \frac{B_j\big((B_j w_j - A_j) + \sqrt{N}\big)}{N - (B_j w_j - A_j)^2} = \frac{B_j(A_{j+1} + \sqrt{N})}{N - A_{j+1}^2} = \frac{A_{j+1} + \sqrt{N}}{B_{j+1}} = w_{j+1}'.
\end{aligned}$$

This implies that

$$w_j' = w_j + \frac{1}{w_{j+1}'} \qquad \text{for } j \geq 0.$$

Since $w_0' = \alpha$, it follows by induction that w_j' is the jth complete quotient and w_j is the jth partial quotient of the simple continued fraction for α. We henceforth use the usual notation q_j' and q_j for these.

Note that we might have $B_0 < 0$. Next, we show that if j is sufficiently large, then $B_j > 0$. Using $\alpha = [q_0, q_1, \dots, q_{n-1}, q_n']$ and the notation of Theorem 12, we obtain

$$\frac{A_0 + \sqrt{N}}{B_0} = \alpha = \frac{q_n' a_{n-1} + a_{n-2}}{q_n' b_{n-1} + b_{n-2}} = \frac{\left(\dfrac{A_n + \sqrt{N}}{B_n}\right) a_{n-1} + a_{n-2}}{\left(\dfrac{A_n + \sqrt{N}}{B_n}\right) b_{n-1} + b_{n-2}}.$$

The lemma now implies (think about it)

$$\frac{A_0 - \sqrt{N}}{B_0} = \frac{\left(\dfrac{A_n - \sqrt{N}}{B_n}\right) a_{n-1} + a_{n-2}}{\left(\dfrac{A_n - \sqrt{N}}{B_n}\right) b_{n-1} + b_{n-2}}.$$

Solving for $(A_n - \sqrt{N})/B_n$, we deduce

$$\frac{A_n - \sqrt{N}}{B_n} = \frac{a_{n-2} - \left(\dfrac{A_0 - \sqrt{N}}{B_0}\right) b_{n-2}}{b_{n-1}\left(\dfrac{A_0 - \sqrt{N}}{B_0}\right) - a_{n-1}} = -\frac{b_{n-2}}{b_{n-1}} \left(\frac{\dfrac{A_0 - \sqrt{N}}{B_0} - \dfrac{a_{n-2}}{b_{n-2}}}{\dfrac{A_0 - \sqrt{N}}{B_0} - \dfrac{a_{n-1}}{b_{n-1}}} \right).$$

As n tends to infinity, the last expression in parentheses approaches 1 (each of the numerator and denominator tends to $(A_0 - \sqrt{N})/B_0 - (A_0 + \sqrt{N})/B_0 = -2\sqrt{N}/B_0$). For n sufficiently large, say $n \geq M$, it follows that $(A_n - \sqrt{N})/B_n < 0$. Therefore, for $n \geq M$,

$$\frac{2\sqrt{N}}{B_n} = \frac{A_n + \sqrt{N}}{B_n} - \frac{A_n - \sqrt{N}}{B_n} = q_n' - \frac{A_n - \sqrt{N}}{B_n} > 0,$$

which implies $B_n > 0$.

Now, by $(*)$, we obtain

$$0 < B_n B_{n+1} = N - A_{n+1}^2 \leq N \qquad \text{for } n \geq M.$$

This implies

$$0 < B_n \leq N \quad \text{ and } \quad |A_{n+1}| < \sqrt{N} \qquad \text{for } n \geq M.$$

Thus, there are only finitely many distinct values of q_n' for $n \geq M+1$, and it follows that $q_{n+r}' = q_n'$ for some positive integers n and r (and, in fact, we can take $r \leq N(2\sqrt{N}+1)$). Hence, $\alpha = [q_0, q_1, \ldots, q_{n-1}, q_n'] = [q_0, q_1, \ldots, q_{n-1}, q_n, \ldots, q_{n+r-1}, q_n'] = [q_0, q_1, \ldots, q_{n-1}, \overline{q_n, \ldots, q_{n+r-1}}]$, completing the proof of the theorem. ■

- On the diophantine equation $x^2 - Ny^2 = B$.

Theorem 29. *Let N be a positive integer which is not a square, and let a_j and b_j be defined, as in Theorem 12, from the simple continued fraction for $\sqrt{N}$. Let B_n be defined as in $(*)$ in the proof of Theorem 28 with $\alpha = \sqrt{N}$. Then for every non-negative integer n, we have $a_{n-1}^2 - N b_{n-1}^2 = (-1)^n B_n$.*

Comment: In the proof of Theorem 28 with $\alpha = \sqrt{N}$, we have $A_0 = 0$ and $B_0 = 1$. Then $(*)$ is used recursively to define B_j for $j \geq 1$.

Proof. Write $\sqrt{N} = [q_0, q_1, \ldots, q_{n-1}, q_n']$ where in $(*)$ $w_j = q_j$ for $0 \leq j \leq n-1$ and $w_n' = q_n'$. We deduce from Theorem 12 and $(*)$ that

$$\sqrt{N} = \frac{q_n' a_{n-1} + a_{n-2}}{q_n' b_{n-1} + b_{n-2}} = \frac{(A_n + \sqrt{N}) a_{n-1} + B_n a_{n-2}}{(A_n + \sqrt{N}) b_{n-1} + B_n b_{n-2}}$$

which implies

$$N b_{n-1} + (A_n b_{n-1} + B_n b_{n-2})\sqrt{N} = (A_n a_{n-1} + B_n a_{n-2}) + a_{n-1}\sqrt{N}.$$

Since $\sqrt{N}$ is irrational,

$$A_n b_{n-1} + B_n b_{n-2} = a_{n-1} \qquad \text{and} \qquad A_n a_{n-1} + B_n a_{n-2} = N b_{n-1}.$$

We deduce that

$$a_{n-1}^2 - N b_{n-1}^2 = B_n(a_{n-1}b_{n-2} - a_{n-2}b_{n-1}),$$

and the result follows from Theorem 12. ■

Recall that, for n sufficiently large, $0 < B_n \le N$. Thus, Theorem 29 gives us a method for obtaining some solutions to diophantine equations of the form $x^2 - Ny^2 = B$ when $|B| \le N$. Our next result shows us that at least in the case $|B| \le \sqrt{N}$, all the solutions can be obtained this way.

Theorem 30. *Let N be a positive integer which is not a square, and let a_j and b_j be defined, as in Theorem 12, from the simple continued fraction for $\sqrt{N}$. Let $q'_n = (A_n + \sqrt{N})/B_n$ be defined as in (∗) (so $w'_n = q'_n$). Suppose a and b are positive relatively prime integers satisfying $a^2 - Nb^2 = B$ for some integer B with $|B| \le \sqrt{N}$. Then there is a positive intger n such that $a = a_{n-1}$, $b = b_{n-1}$, and $B = (-1)^n B_n$.*

Proof. Suppose first that $0 < B \le \sqrt{N}$. Momentarily, we suppose only that B and N are in $\mathbb{R}^+$ (in other words, we do not require them to be positive integers). Since $a^2 - Nb^2 = B$, we obtain

$$\frac{a}{b} - \sqrt{N} = \frac{B}{\left(\frac{a}{b} + \sqrt{N}\right)b^2} > 0.$$

Hence,

$$\left|\frac{a}{b} - \sqrt{N}\right| < \frac{\sqrt{N}}{2\sqrt{N}b^2} = \frac{1}{2b^2}.$$

The condition that $\gcd(a, b) = 1$ and Theorem 23 imply that $a = a_{n-1}$ and $b = b_{n-1}$ for some $n \ge 1$. If we now restrict our attention to $N \in \mathbb{Z}^+$, we deduce from Theorem 29 that $B = (-1)^n B_n$.

Since $\sqrt{N}$ is not rational, it remains to consider the case that $-\sqrt{N} \le B < 0$. Here, we use that $a^2 - Nb^2 = B$ implies $b^2 - (1/N)a^2 = -B/N > 0$. By what we just established, we deduce that b/a is a convergent of the simple continued fraction for $1/\sqrt{N}$. If $\sqrt{N} = [q_0, q_1, \dots]$, then $1/\sqrt{N} = [0, q_0, q_1, \dots]$. It follows that the nth convergent of the simple continued fraction for $\sqrt{N}$ is the reciprocal of the $(n-1)$st convergent of the simple continued fraction for $1/\sqrt{N}$. Hence, there is an $n \ge 1$ (since a and b are positive) such that $a = a_{n-1}$ and $b = b_{n-1}$. As before, Theorem 29 implies that $B = (-1)^n B_n$. ■

• Units in quadratic extensions revisited. Our next goal is to determine when $B_n = 1$ in developing the simple continued fraction for $\sqrt{N}$. Note that if $B_n = 1$, then (∗) implies that $q'_n = A_n + \sqrt{N}$ so that

$$\sqrt{N} = [q_0, q_1, \dots, q_{n-1}, q'_n] = [q_0, q_1, \dots, q_{n-1}, A_n + \sqrt{N}] = [q_0, \overline{q_1, \dots, q_{n-1}, A_n + q_0}].$$

Thus, if $B_n = 1$, then the simple continued fraction for $\sqrt{N}$ can be expressed as a periodic simple continued fraction with the periodic part beginning with the first partial quotient (i.e., q_1) and ending with the nth partial quotient. We show that the converse of this statement also holds. More precisely, we show that given a non-square integer $N > 1$, we have $\sqrt{N} = [q_0, \overline{q_1, \dots, q_{n-1}, q_n}]$ and, for any such representation, $B_n = 1$.

Lemma 1. *Let β be an irrational number that is a root of a quadratic polynomial in $\mathbb{Z}[x]$, and let $\overline{\beta}$ be the other (necessarily irrational) root. Then the simple continued fraction for β is purely periodic if and only if $\beta > 1$ and $\overline{\beta} \in (-1, 0)$.*

Proof. Suppose first that the simple continued fraction for β is purely periodic, and write $\beta = [\overline{q_0, q_1, \dots, q_n}]$. Observe that we necessarily have $q_j \geq 1$ for all $j \geq 0$. Hence, $\beta > 1$. We have already seen that β satisfies the quadratic $b_n x^2 + (b_{n-1} - a_n)x - a_{n-1}$. The irrational number $\overline{\beta}$ is the other root of this quadratic, and we deduce from the Intermediate Value Theorem that it is in $(-1, 0)$.

Now, suppose we know $\beta > 1$ and $\overline{\beta} \in (-1, 0)$ and we want to prove β is purely periodic. Writing $\beta = [q_0, q_1, \dots]$ and using the notation from the proof of Theorem 28, we show by induction that the number $\overline{q'_j} = (A_j - \sqrt{N})/B_j$ is in $(-1, 0)$. For $j = 0$, this is clear. Observe that $\beta > 1$ implies $q_j \geq 1$ for all $j \geq 0$. If $\overline{q'_j} \in (-1, 0)$, we use that

$$q'_j = q_j + \frac{1}{q'_{j+1}} \qquad \Longrightarrow \qquad \overline{q'_j} = q_j + \frac{1}{\overline{q'_{j+1}}}$$

to finish the induction argument by establishing that $\overline{q'_{j+1}} \in (-1, 0)$.

Using that $\overline{q'_j} = q_j + (1/\overline{q'_{j+1}}) \in (-1, 0)$, we deduce that

$$-\frac{1}{\overline{q'_{j+1}}} - 1 < q_j < -\frac{1}{\overline{q'_{j+1}}} \qquad \Longrightarrow \qquad q_j = \left[-\frac{1}{\overline{q'_{j+1}}} \right] \qquad \text{for } j \geq 0.$$

On the other hand, from the proof of Theorem 28, $\overline{q'_j} = (A_j - \sqrt{N})/B_j$ is eventually periodic. Hence, we can find non-negative integers k and ℓ, with k minimal and $\ell \neq k$, such that $\overline{q'_k} = \overline{q'_\ell}$. The observations that

$$q_{k-1} = \left[-\frac{1}{\overline{q'_k}} \right] = \left[-\frac{1}{\overline{q'_\ell}} \right] = q_{\ell-1} \quad \text{and} \quad \overline{q'_{k-1}} = q_{k-1} + \frac{1}{\overline{q'_k}} = q_{\ell-1} + \frac{1}{\overline{q'_\ell}} = \overline{q'_{\ell-1}}$$

imply $k = 0$. It follows that $q'_\ell = q'_0$ from which we deduce that β is purely periodic. ■

Lemma 2. *Let β be a quadratic irrational, and let $q'_j = (A_j + \sqrt{N})/B_j$ be the complete quotients associated with the simple continued fraction for β. If β is purely periodic, then $B_j > 0$ for all $j \geq 0$.*

Proof. In the proof of Lemma 1, we saw that $\overline{q'_j} < 0$ for all $j \geq 0$. The result follows now by considering $q'_j - \overline{q'_j}$ as in the final arguments in the proof of Theorem 28. ■

Theorem 31. *Let N be a positive integer which is not a square. There is a minimal positive integer n and positive integers $q_0, q_1, \ldots, q_{n-1}$ for which*

$$(*) \qquad \sqrt{N} = [q_0, \overline{q_1, \ldots, q_{n-1}, 2q_0}].$$

Furthermore, if the jth complete quotient of $\sqrt{N}$ is $q_j' = (A_j + \sqrt{N})/B_j$, then $B_j > 0$ for all $j \geq 0$ and $B_j = 1$ if and only if n divides j.

Proof. Let $q_0 = [\sqrt{N}]$, and let $\beta = q_0 + \sqrt{N} = [\sqrt{N}] + \sqrt{N}$. Then $\overline{\beta} = q_0 - \sqrt{N} \in (-1, 0)$; hence, by Lemma 1, β is purely periodic. Note that $[\beta] = [q_0 + \sqrt{N}] = q_0 + [\sqrt{N}] = 2q_0$. Thus, there are positive integers $q_1, q_2, \ldots, q_{n-1}$ for which

$$\beta = q_0 + \sqrt{N} = [\overline{2q_0, q_1, \ldots, q_{n-1}}] = [2q_0, \overline{q_1, \ldots, q_{n-1}, 2q_0}].$$

It follows that $(*)$ holds (and we may take n to be minimal). Observe that the complete quotients q_j' for β and for $\sqrt{N}$ are the same for $j \geq 1$. It follows from Lemma 2 that $B_j \geq 1$ for all $j \geq 0$.

Since $q_n' = [\overline{2q_0, q_1, \ldots, q_{n-1}}] = q_0 + \sqrt{N}$, we deduce that $B_n = 1$. Also, $q_{kn}' = q_n'$ for all positive integers k so that $B_j = 1$ if n divides j (this is even true for $j = 0$). Also, if $B_j = 1$, then

$$\sqrt{N} = [q_0, q_1, \ldots, q_{j-1}, A_j + \sqrt{N}] = [q_0, \overline{q_1, \ldots, q_{j-1}, A_j + q_0}].$$

We want to show that n divides j, and we may suppose that $j \geq 1$ and do so. We deduce that $q_j' = A_j + \sqrt{N}$ is a complete quotient for $\beta = q_0 + \sqrt{N}$ as well as $\sqrt{N}$. Since β is purely periodic, we deduce from the proof of Lemma 1 that $\overline{q_j'} = A_j - \sqrt{N} \in (-1, 0)$. Therefore, $\sqrt{N} - 1 < A_j < \sqrt{N}$, and $A_j = [\sqrt{N}] = q_0$. Hence, $\sqrt{N} = [q_0, \overline{q_1, \ldots, q_{j-1}, 2q_0}]$. We deduce that $j \geq n$, and for $1 \leq i \leq n-1$, $B_i \geq 2$. Since $q_{kn+i}' = q_i'$ for $1 \leq i \leq n$ and k a positive integer, we see that if $B_j = 1$, then n divides j. ■

Theorem 32. *Let N be a positive integer which is not a square. The solutions of $x^2 - Ny^2 = \pm 1$ are given by $(x, y) = (\pm a_{kn-1}, b_{kn-1})$ and $(x, y) = (\pm a_{kn-1}, -b_{kn-1})$ where k is a non-negative integer and n is the minimal positive integer such that $(*)$ holds for some positive integers $q_0, q_1, \ldots, q_{n-1}$. (Here a_j and b_j are as defined in Theorem 12.)*

Proof. Combine Theorems 29, 30, and 31. ■

Theorem 33. *Let N be a positive integer which is not a square. Let x_1 and y_1 be positive integers for which $x_1^2 - Ny_1^2 = \pm 1$ and $x_1 + y_1\sqrt{N}$ is as small as possible. Then the solutions to $x^2 - Ny^2 = \pm 1$ with x and y positive intgers are precisely given by $(x, y) = (x_j, y_j)$ where j is a positive integer and $x_j + y_j\sqrt{N} = (x_1 + y_1\sqrt{N})^j$.*

Proof. Let x_0 and y_0 be positive integers satisfying $x_0^2 - Ny_0^2 = \pm 1$. Then $x_0 + y_0\sqrt{N}$ is a unit in $\mathbb{Z}[\sqrt{N}]$. Also, $x_1 + y_1\sqrt{N}$ is a unit in $\mathbb{Z}[\sqrt{N}]$. Let m be the positive integer for which $(x_1 + y_1\sqrt{N})^m \leq x_0 + y_0\sqrt{N} \leq (x_1 + y_1\sqrt{N})^{m+1}$. Let

$$a + b\sqrt{N} = (x_0 + y_0\sqrt{N})(x_1 + y_1\sqrt{N})^{-m}.$$

Then $a+b\sqrt{N} \in [1, x_1+y_1\sqrt{N})$ and $a^2 - Nb^2 = \pm 1$. Observe that if $a+b\sqrt{N} = 1$, then $x_0 + y_0\sqrt{N} = (x_1+y_1\sqrt{N})^m$ and we are through. Assume now that $a+b\sqrt{N} \neq 1$. Then $a+b\sqrt{N} > 1$, and we obtain $|a-b\sqrt{N}| = 1/(a+b\sqrt{N}) < 1$. Thus, $-1 < a-b\sqrt{N} < 1$. Now, $a+b\sqrt{N} > 1$ implies $a > 0$ and $b > 0$. Since $a+b\sqrt{N} < x_1+y_1\sqrt{N}$, the minimality condition on $x_1+y_1\sqrt{N}$ now gives a contradiction. The theorem follows. ■

Comment: If N is squarefree and $N \not\equiv 1 \pmod 4$, then the number $x_1+y_1\sqrt{N}$ is called the *fundamental unit* for the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. Theorem 33 implies that the fundamental unit generates all units in the ring in the sense that the units are given by $\pm(x_1+y_1\sqrt{N})^m$ where m denotes an arbitrary integer.

• An example. Suppose we want the "minimal" solution to the equation $x^2 - 89y^2 = 1$ in positive integers x and y. We compute $\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}]$. We know that the solutions of $x^2 - 89y^2 = 1$ come from considering positive integers k in the equation $a_{kn-1}^2 - 89b_{kn-1}^2 = (-1)^{kn}$ where $n = 5$ (see Theorems 29, 31, and 32). Thus, the smallest solution will occur when we take $k = 2$, $x = a_9$, and $y = b_9$. This gives $x = 500001$ and $y = 53000$.

Homework:

(1) Beginning with $x_0 = 1$ as an approximation to $\sqrt{2}$, use Newton's method (from Calculus) to compute better approximations $x_1, x_2, \ldots$ to $\sqrt{2}$. Prove that these approximations are all convergents of the simple continued fraction for $\sqrt{2}$.

(2) Find the three "smallest" positive integer solutions to $x^2 - 29y^2 = 1$.

(3) Consider the integers $n \geq 2$ such that $\binom{n}{2}$ is a square. The first such integer is 2 since $\binom{2}{2} = 1^2$. The second such integer is 9 and $\binom{9}{2} = 6^2$. Find the third, fourth, and fifth such integers. Your answer should be obtained without using a calculator or computer, and all work should be shown.

Algebraic Number Fields Revisited:

• Some preliminaries. If α is an algebraic number, its minimal polynomial $f(x)$ is clearly irreducible. If α' is another root of $f(x)$, then the lemma to Theorem 28 implies that the minimal polynomial for α' divides $f(x)$. It follows that $f(x)$ is also the minimal polynomial for α'. In other words, we have

Theorem 34. *Let $f(x)$ be the minimal polynomial for α, and let $\alpha_2, \alpha_3, \ldots, \alpha_n$ be the other roots of $f(x)$. Then $f(x)$ is irreducible and $f(x)$ is also the minimal polynomial for $\alpha_2, \alpha_3, \ldots, \alpha_n$.*

The next result was a previous homework assignment established by "rationalizing the denominator," but here we give an easier approach.

Theorem 35. *Let α be an algebraic number with minimal polynomial $f(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$. Every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely in the form $g(\alpha)$ where $g(x) \in \mathbb{Q}[x]$ with $g(x) \equiv 0$ or $\deg g(x) \leq n-1$.*

Proof. Fix $\beta \in \mathbb{Q}(\alpha)$. We showed earlier that there are $N(x)$ and $D(x)$ in $\mathbb{Q}[x]$ such that $\deg D(x) \le n-1$, $D(\alpha) \ne 0$, and $\beta = N(\alpha)/D(\alpha)$ (we said more, but this is all we want here). We take such an $N(x)$ and $D(x)$ with $D(x)$ of minimal degree. Clearly, $\deg D(x) \le n-1$. We want to show now that $\deg D(x) = 0$. Assume $\deg D(x) \ge 1$ and note that $\deg D(x) < \deg f(x)$. Since $f(x)$ is irreducible, we know that $D(x) \nmid f(x)$. Hence, there exist non-zero polynomials $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $f(x) = q(x)D(x) + r(x)$ and $0 \le \deg r(x) < \deg D(x)$. Observe that $\deg r(x) < n-1$ and the minimal polynomial of α having degree n imply that $r(\alpha) \ne 0$. On the other hand,

$$r(\alpha) = f(\alpha) - q(\alpha)D(\alpha) = -q(\alpha)D(\alpha) \qquad \Longrightarrow \qquad \beta = \frac{N(\alpha)}{D(\alpha)} = \frac{-q(\alpha)N(\alpha)}{r(\alpha)}.$$

Since $\deg r(x) < \deg D(x)$, we obtain a contradiction to the minimality of $\deg D(x)$. We deduce that $\beta = g(\alpha)$ for some $g(x) \in \mathbb{Q}[x]$. That we may take $\deg g(x) \le n-1$ follows in the same manner we established earlier in the notes that $\deg D(x) \le n-1$ in the representation for β above. If there were two such $g(x)$, then a constant times their difference would be a monic polynomial of degree $\le n-1$ having α as a root. This would be impossible since $\deg f = n$ and $f(x)$ is the minimal polynomial for α. Thus, for a given β, such a $g(x)$ is unique. ■

• More general fields? We have defined algebraic number fields to be fields of the form $\mathbb{Q}(\alpha)$ where α is an algebraic number. It is reasonable to consider instead $\mathbb{Q}(\alpha_1', \alpha_2', \dots, \alpha_r')$ defined as the smallest field containing $\mathbb{Q}$ and some algebraic numbers $\alpha_1', \alpha_2', \dots, \alpha_r'$. Observe that $\mathbb{Q}(\alpha_1', \alpha_2', \dots, \alpha_r') = \mathbb{Q}(\alpha_1', \alpha_2', \dots, \alpha_{r-1}')(\alpha_r')$, the smallest field which contains $\mathbb{Q}(\alpha_1', \alpha_2', \dots, \alpha_{r-1}')$ and α_r' (this equality should be justified). We show that in fact such a field is an algebraic number field.

Theorem 36. *Let $\alpha_1', \alpha_2', \dots, \alpha_r'$ be any algebraic numbers. Then there exists an algebraic number γ such that $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1', \alpha_2', \dots, \alpha_r')$.*

Proof. It suffices to show that if α and β are algebraic, then there exists an algebraic number γ for which $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$. Let $\alpha_1 = \alpha$ and $\alpha_2, \dots, \alpha_n$ be the distinct roots of the minimal polynomial $f(x)$ for α; and let $\beta_1 = \beta$ and $\beta_2, \dots, \beta_m$ be the distinct roots of the minimal polynomial $g(x)$ for β. Note that for $i \in \{1, 2, \dots, n\}$ and $j \in \{2, 3, \dots, m\}$, there exists a unique $x = x(i,j)$ such that $\alpha_i + x\beta_j = \alpha + x\beta$. It follows that there is a rational number c for which the number $\gamma = \alpha + c\beta$ satisfies

$$\gamma \ne \alpha_i + c\beta_j \quad \text{ for all } i \in \{1, 2, \dots, n\} \text{ and } j \in \{2, 3, \dots, m\}.$$

We prove $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$.

To prove $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$, we show that $\gamma \in \mathbb{Q}(\alpha, \beta)$ and that each of α and β is in $\mathbb{Q}(\gamma)$. Clearly, $\gamma \in \mathbb{Q}(\alpha, \beta)$. Let $h(x) = f(\gamma - cx) \in \mathbb{Q}(\gamma)[x]$. Note that $h(\beta) = f(\alpha) = 0$. On the other hand, by our choice of c, we have $h(\beta_j) \ne 0$ for each $j \in \{2, 3, \dots, m\}$. Using the Euclidean algorithm, we obtain $w(x) = \gcd(g(x), h(x)) \in \mathbb{Q}(\gamma)[x]$ (where we consider $w(x)$ monic). Since $g(x)$ is irreducible, β is a root of $g(x)$ with multiplicity one. Since β is the only root $g(x)$ and $h(x)$ have in common, it follows that $w(x) = x + a$ with $w(\beta) = 0$.

Since $w(x) \in \mathbb{Q}(\gamma)[x]$, we deduce that $\beta = -a \in \mathbb{Q}(\gamma)$. Hence, $\alpha = \gamma - c\beta \in \mathbb{Q}(\gamma)$. This completes the proof. ∎

Conjugates of Algebraic Numbers:

• Definitions. Let β be an algebraic number with minimum polynomial $g(x)$. The roots of $g(x)$ are called the *conjugates of* β. Suppose $\beta \in \mathbb{Q}(\alpha)$ where α is an algebraic number with minimum polynomial $f(x)$. If $\deg f = n$, then we can find $h(x) \in \mathbb{Q}[x]$, with $h(x) \equiv 0$ or $\deg h \le n-1$, such that $\beta = h(\alpha)$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be the n roots of $f(x)$, and let $\beta_1 = \beta, \beta_2, \dots, \beta_m$ be the roots of $g(x)$. Thus, $\beta_1, \dots, \beta_m$ are the conjugates of β. The numbers $h(\alpha_1), h(\alpha_2), \dots, h(\alpha_n)$ are called the *field conjugates of* β *in* $\mathbb{Q}(\alpha)$. This terminology is not as misleading as it may seem as the following theorem shows.

Theorem 37. *Given the notation above, $m|n$ and $h(\alpha_1), \dots, h(\alpha_n)$ is some arrangement of n/m copies of $\beta_1, \dots, \beta_m$. In other words, if $F(x) = \prod_{j=1}^{n}(x - h(\alpha_j))$, then $F(x) = g(x)^{n/m}$. Also, if $F(x) = g(x)$ (i.e., if $n = m$), then $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.*

Proof. Since $F(x)$ is symmetric in $\alpha_1, \dots, \alpha_n$, we deduce that $F(x) \in \mathbb{Q}[x]$. We write

$$F(x) = f_1(x) f_2(x) \cdots f_r(x)$$

where each $f_j(x)$ is a monic irreducible polynomial in $\mathbb{Q}[x]$. We also take $f_1(x)$ so that $f_1(h(\alpha)) = 0$. Thus, $f_1(\beta) = 0$. Since both $g(x)$ and $f_1(x)$ are monic irreducible polynomials with $g(\beta) = f_1(\beta) = 0$, we obtain $f_1(x) = g(x)$.

Each remaining $f_j(x)$ has some (not necessarily the same) $h(\alpha_i)$ as a root. Note that $f_j(h(\alpha_i)) = 0$ implies that α_i is a root of $f_j(h(x))$. But this implies that $f(x)$ divides $f_j(h(x))$ so that $f_j(h(\alpha)) = 0$. As with $f_1(x)$, we deduce that $f_j(x) = g(x)$. Hence, we obtain $F(x) = g(x)^r$. Comparing degrees, we get that $r = n/m$.

Now, suppose $n = m$ so that $F(x) = g(x)$. Since we know that $\beta \in \mathbb{Q}(\alpha)$, it suffices to show that $\alpha \in \mathbb{Q}(\beta)$ to establish that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Note that

$$G(x) = F(x) \sum_{j=1}^{n} \frac{\alpha_j}{x - h(\alpha_j)}$$

is a symmetric polynomial in $\alpha_1, \dots, \alpha_n$ so that $G(x) \in \mathbb{Q}[x]$. Observe that

$$G(\beta) = G(h(\alpha)) = \alpha F'(h(\alpha)) = \alpha F'(\beta).$$

Since β is a root of $g(x)$ with multiplicity one, we have $F'(\beta) = g'(\beta) \neq 0$. We deduce $\alpha = G(\beta)/F'(\beta) \in \mathbb{Q}(\beta)$, and the theorem follows. ∎

Comment: The polynomial $F(x)$ in Theorem 37 is called the *field polynomial for* β.

A lemma about conjugates that we will use momentarily is:

Lemma. *Given the notation above, let $w(x) \in \mathbb{Q}[x]$ with $\beta = w(\alpha)$ (we do not require $\deg w \le n-1$). Then, for each $j \in \{1, 2, \dots, n\}$, the field conjugate $\beta_j = h(\alpha_j)$ satisfies $\beta_j = w(\alpha_j)$.*

Proof. Divide $w(x)$ by $f(x)$ (the minimal polynomial for α) to get $w(x) = f(x)q(x) + r(x)$ where $q(x)$ and $r(x)$ are in $\mathbb{Q}[x]$ with $r(x) \equiv 0$ or $\deg r \le n-1$. Then $\beta = w(\alpha) = r(\alpha)$ so that, in fact, $r(x) = h(x)$. The result follows now since

$$w(\alpha_j) = f(\alpha_j)q(\alpha_j) + r(\alpha_j) = r(\alpha_j) = h(\alpha_j)$$

for each $j \in \{1, 2, \dots, n\}$. ■

• Norms and traces. Let $\beta \in \mathbb{Q}(\alpha)$ (where α is an algebraic number), and let $\beta_1, \beta_2, \dots, \beta_n$ be the field conjugates of β. Then the norm of β is defined to be

$$N(\beta) = N_{\mathbb{Q}(\alpha)}(\beta) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta) = \beta_1\beta_2\cdots\beta_n,$$

and the trace of β is defined to be

$$Tr(\beta) = Tr_{\mathbb{Q}(\alpha)}(\beta) = Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta) = \beta_1 + \beta_2 + \cdots + \beta_n.$$

Note that if $F(x) = \sum_{j=0}^{n} a_j x^j$ is the field polynomial for β (so that $a_n = 1$), then

$$N(\beta) = (-1)^n a_0 \quad \text{and} \quad Tr(\beta) = -a_{n-1}.$$

Also, if $g(x) = \sum_{j=0}^{m} b_j x^j$ is the minimal polynomial for β as in Theorem 37 with roots $\beta_1, \dots, \beta_m$, then

$$N(\beta) = (\beta_1\cdots\beta_m)^{n/m} = (-1)^n b_0^{n/m} \quad \text{and} \quad Tr(\beta) = \frac{n}{m}(\beta_1+\beta_2+\cdots+\beta_m) = -\frac{n}{m} b_{m-1}.$$

Theorem 38. *Let β and γ be in $\mathbb{Q}(\alpha)$. Then*

$$N(\beta\gamma) = N(\beta)N(\gamma) \quad \textit{and} \quad Tr(\beta+\gamma) = Tr(\beta) + Tr(\gamma).$$

Proof. Let n be the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ (defined as the degree of the minimal polynomial for α). Then there are unique rational numbers $b_0, \dots, b_{n-1}$ and $c_0, \dots, c_{n-1}$ such that

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \quad \text{and} \quad \gamma = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

Clearly,

$$\beta + \gamma = \sum_{j=0}^{n-1} (b_j + c_j)\alpha^j$$

so that if $\alpha_1, \alpha_2, \dots, \alpha_n$ are the conjugates of α, then

$$Tr(\beta+\gamma) = \sum_{i=1}^{n} \Big(\sum_{j=0}^{n-1} (b_j + c_j)\alpha_i^j \Big) = \sum_{i=1}^{n} \Big(\sum_{j=0}^{n-1} b_j\alpha_i^j \Big) + \sum_{i=1}^{n} \Big(\sum_{j=0}^{n-1} c_j\alpha_i^j \Big) = Tr(\beta) + Tr(\gamma).$$

Set $g(x) = \sum_{j=0}^{n-1} b_j x^j$ and $h(x) = \sum_{j=0}^{n-1} c_j x^j$. Then $g(\alpha_1), \dots, g(\alpha_n)$ are the field conjugates of β, and $h(\alpha_1), \dots, h(\alpha_n)$ are the field conjugates of γ. Let $w(x) = g(x)h(x) \in \mathbb{Q}[x]$ so that $\beta\gamma = w(\alpha)$. Then the last lemma implies

$$N(\beta\gamma) = w(\alpha_1)\cdots w(\alpha_n) = g(\alpha_1)h(\alpha_1)\cdots g(\alpha_n)h(\alpha_n) = N(\beta)N(\gamma),$$

completing the proof. ■

Theorem 39. *Let $\beta \in \mathbb{Q}(\alpha)$. Then $N(\beta) \in \mathbb{Q}$ and $Tr(\beta) \in \mathbb{Q}$. If β is an algebraic integer, then $N(\beta) \in \mathbb{Z}$ and $Tr(\beta) \in \mathbb{Z}$.*

Homework:

(1) (a) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(b) Since $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, there is an $h(x) \in \mathbb{Q}[x]$ such that $\sqrt{2} = h(\sqrt{2}+\sqrt{3})$. Find such an $h(x)$.

(c) What is the field polynomial for $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Simplify your answer.

(d) Calculate $N_{\mathbb{Q}(\sqrt{2}+\sqrt{3})}(\sqrt{2})$ and $Tr_{\mathbb{Q}(\sqrt{2}+\sqrt{3})}(\sqrt{2})$.

(2) Prove Theorem 39.

Discriminants and Integral Bases:

• Definition. Let α be an algebraic number with conjugates $\alpha_1, \dots, \alpha_n$. Let $\beta^{(1)}, \dots, \beta^{(n)} \in \mathbb{Q}(\alpha)$. For each $i \in \{1, \dots, n\}$, let $h_i(x) \in \mathbb{Q}[x]$ be such that $\beta^{(i)} = h_i(\alpha)$ and $h_i(x) \equiv 0$ or $\deg h_i \le n-1$. For each i and j in $\{1, \dots, n\}$, let $\beta_j^{(i)} = h_i(\alpha_j)$. The *discriminant of* $\beta^{(1)}, \dots, \beta^{(n)}$ is defined by

$$\Delta(\beta^{(1)}, \dots, \beta^{(n)}) = \big(\det(\beta_j^{(i)})\big)^2.$$

Observe that the ordering of the conjugates $\alpha_1, \dots, \alpha_n$ of α as well as the ordering of $\beta^{(1)}, \dots, \beta^{(n)}$ does not affect the value of the discriminant. On the other hand, the ordering on the conjugates of the $\beta^{(i)}$ is important (if $\beta_j^{(1)} = h_1(\alpha_j)$, then we want the jth conjugate of each $\beta^{(i)}$ to be determined by plugging in α_j into $h_i(x)$).

Theorem 40. *If $\beta^{(1)}, \dots, \beta^{(n)} \in \mathbb{Q}(\alpha)$, then $\Delta(\beta^{(1)}, \dots, \beta^{(n)}) \in \mathbb{Q}$. If $\beta^{(1)}, \dots, \beta^{(n)}$ are algebraic integers, then $\Delta(\beta^{(1)}, \dots, \beta^{(n)}) \in \mathbb{Z}$.*

Proof. This follows from Theorem 39 since

$$\Delta(\beta^{(1)}, \dots, \beta^{(n)}) = \det \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \dots & \beta_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \beta_2^{(n)} & \dots & \beta_n^{(n)} \end{pmatrix} \det \begin{pmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \dots & \beta_1^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_n^{(1)} & \beta_n^{(2)} & \dots & \beta_n^{(n)} \end{pmatrix}$$

$$= \det\big(\beta_1^{(i)}\beta_1^{(j)} + \beta_2^{(i)}\beta_2^{(j)} + \cdots + \beta_n^{(i)}\beta_n^{(j)}\big) = \det\big(Tr(\beta^{(i)}\beta^{(j)})\big),$$

where the last equation follows from an application of the last lemma. ∎

• Integral bases. The numbers $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ form a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. It follows that every bases for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ consists of n elements. Let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. We next seek to find a basis for R over $\mathbb{Z}$. Such a basis is called an *integral basis* (in $\mathbb{Q}(\alpha)$). Theorem 6 implies that every integral basis in $\mathbb{Q}(\alpha)$ is a basis for $\mathbb{Q}(\alpha)$. Note that an integral basis is not defined as a basis for $\mathbb{Q}(\alpha)$ consisting of algebraic integers from the field (for example, $\{1, \sqrt{5}\}$ would be such a basis for $\mathbb{Q}(\sqrt{5})$ but it is not an integral basis).

Lemma. *Let $\mathbb{Q}(\alpha)$ be an algebraic extension of $\mathbb{Q}$ of degree n. Suppose $\beta^{(1)}, \dots, \beta^{(n)}$ and $\gamma^{(1)}, \dots, \gamma^{(n)}$ in $\mathbb{Q}(\alpha)$ are related by the matrix equation*

$$\begin{pmatrix} \beta^{(1)} \\ \beta^{(2)} \\ \vdots \\ \beta^{(n)} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \gamma^{(1)} \\ \gamma^{(2)} \\ \vdots \\ \gamma^{(n)} \end{pmatrix},$$

where the a_{ij} are rational numbers. Then

$$\Delta(\beta^{(1)}, \dots, \beta^{(n)}) = \det \big(a_{ij}\big)^2 \Delta(\gamma^{(1)}, \dots, \gamma^{(n)}).$$

Proof. For $i \in \{1, 2, \dots, n\}$, let $h_i(x) \in \mathbb{Q}[x]$ denote the polynomial of degree $\le n-1$ such that $\gamma^{(i)} = h_i(\alpha)$. Then the matrix equation implies that $\beta^{(i)} = g_i(\alpha)$ where $g_i(x) = a_{i1}h_1(x) + \cdots + a_{in}h_n(x) \in \mathbb{Q}[x]$ for $1 \le i \le n$. It follows that

$$\begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \dots & \beta_n^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} & \dots & \beta_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \beta_2^{(n)} & \dots & \beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \gamma_1^{(1)} & \gamma_2^{(1)} & \dots & \gamma_n^{(1)} \\ \gamma_1^{(2)} & \gamma_2^{(2)} & \dots & \gamma_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{(n)} & \gamma_2^{(n)} & \dots & \gamma_n^{(n)} \end{pmatrix}.$$

Taking determinants and squaring, the result follows. ■

Theorem 41. *Let $\mathbb{Q}(\alpha)$ be an algebraic extension of $\mathbb{Q}$ of degree n. Let $\omega^{(1)}, \dots, \omega^{(n)}$ be n algebraic integers in $\mathbb{Q}(\alpha)$ with $|\Delta(\omega^{(1)}, \dots, \omega^{(n)})| > 0$ as small as possible. Then $\omega^{(1)}, \dots, \omega^{(n)}$ form an integral basis in $\mathbb{Q}(\alpha)$.*

Proof. First, we show that $\omega^{(1)}, \dots, \omega^{(n)}$ form a basis for $\mathbb{Q}(\alpha)$. To do this, it suffices to show that $\det \big(a_{ij}\big) \ne 0$ where the numbers a_{ij} are the rational numbers uniquely determined by the equations

$$\omega^{(i)} = \sum_{j=1}^{n} a_{ij}\alpha^{j-1} \qquad \text{for } 1 \le i \le n.$$

By the lemma,

$$\Delta(\omega^{(1)}, \dots, \omega^{(n)}) = \det \big(a_{ij}\big)^2 \Delta(1, \alpha, \dots, \alpha^{n-1}).$$

Since $|\Delta(\omega^{(1)}, \dots, \omega^{(n)})| > 0$, we deduce that $\det \big(a_{ij}\big) \ne 0$. Thus, $\{\omega^{(1)}, \dots, \omega^{(n)}\}$ is a basis for $\mathbb{Q}(\alpha)$.

Now, let β be an algebraic integer in $\mathbb{Q}(\alpha)$. Let $b_1, \dots, b_n$ be rational numbers such that

$$\beta = b_1\omega^{(1)} + b_2\omega^{(2)} + \cdots + b_n\omega^{(n)}.$$

We want to show that each b_i is in $\mathbb{Z}$. Assume otherwise so that for some $k \in \{1, 2, \dots, n\}$, we have $b_k = u + \theta$ where $u \in \mathbb{Z}$ and $0 < \theta < 1$. Define

$$\overline{\omega}^{(k)} = b_1\omega^{(1)} + \cdots + b_{k-1}\omega^{(k-1)} + \theta\omega^{(k)} + b_{k+1}\omega^{(k+1)} + \cdots + b_n\omega^{(n)}$$

and $\overline{\omega}^{(j)} = \omega^{(j)}$ for $j \neq k$ with $1 \leq j \leq n$. Since

$$\det \begin{pmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \ldots & \theta & \ldots & b_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 1 \end{pmatrix} = \theta,$$

the lemma implies that

$$\Delta(\overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)}) = \theta^2 \Delta(\omega^{(1)}, \ldots, \omega^{(n)}).$$

Thus, $0 < |\Delta(\overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)})| < |\Delta(\omega^{(1)}, \ldots, \omega^{(n)})|$. On the other hand, since $\overline{\omega}^{(k)} = \beta - u\omega^{(k)}$, each $\overline{\omega}^{(j)}$ is an algebraic integer for $1 \leq j \leq n$. This contradicts the minimality of $|\Delta(\omega^{(1)}, \ldots, \omega^{(n)})|$, completing the proof. ■

Homework:

(1) Let $\omega^{(1)}, \ldots, \omega^{(n)}$ be an integral basis in $\mathbb{Q}(\alpha)$. Prove that $|\Delta(\omega^{(1)}, \ldots, \omega^{(n)})|$ is > 0 and as small as possible.

(2) Compute $\Delta(1, \alpha)$ where α is a root of $ax^2 + bx + c = 0$ where a, b, and c are in $\mathbb{Z}$ and α is irrational.

Comments and Definitions: By the first problem above, it follows that the discriminants of any two integral bases for a given number field $\mathbb{Q}(\alpha)$ have the same absolute value. Since the discriminants will differ by a square, the signs must also be the same. The common value for the discriminant, denoted Δ, is called *the discriminant of the field* $\mathbb{Q}(\alpha)$. To completely justify that an integral basis (and the discriminant of an algebraic number field) exist, we still need to verify that in any field $\Delta(\omega^{(1)}, \ldots, \omega^{(n)})$ is non-zero for some algebraic numbers $\omega^{(1)}, \ldots, \omega^{(n)}$. This can be done as follows. Consider $\mathbb{Q}(\alpha)$, and use Theorem 6 to obtain a $k \in \mathbb{Z}$ such that $k\alpha \in R$, the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Take $w^{(i)} = k^{i-1}\alpha^{i-1}$ for $1 \leq i \leq n$. It easily follows (by the last lemma) that $\Delta(\omega^{(1)}, \ldots, \omega^{(n)}) = k^{n(n-1)}\Delta(1, \alpha, \ldots, \alpha^{n-1})$. The determinant defining $\Delta(1, \alpha, \ldots, \alpha^{n-1})$ is called a *Van der Monde determinant*, and it will follow by our first lemma below that it is non-zero. This then will imply that $\Delta(\omega^{(1)}, \ldots, \omega^{(n)})$ is non-zero for some algebraic numbers $\omega^{(1)}, \ldots, \omega^{(n)}$ in $\mathbb{Q}(\alpha)$.

Given two bases (not necessarily integral), say $\{\omega^{(1)}, \ldots, \omega^{(n)}\}$ and $\{\overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)}\}$, the values of $\Delta(\omega^{(1)}, \ldots, \omega^{(n)})$ and $\Delta(\overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)})$ differ by the square of a rational number. If the numbers $\omega^{(1)}, \ldots, \omega^{(n)}, \overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)}$ are algebraic integers and $\{\omega^{(1)}, \ldots, \omega^{(n)}\}$ is an integral basis, then $\Delta(\overline{\omega}^{(1)}, \ldots, \overline{\omega}^{(n)}) = k^2\Delta(\omega^{(1)}, \ldots, \omega^{(n)})$ for some $k \in \mathbb{Z}$. Hence, we deduce

Theorem 42. *If $\omega^{(1)}, \dots, \omega^{(n)}$ are algebraic integers in an algebraic number field $\mathbb{Q}(\alpha)$ of degree n over $\mathbb{Q}$ and if $\Delta(\omega^{(1)}, \dots, \omega^{(n)})$ is squarefree, then $\{\omega^{(1)}, \dots, \omega^{(n)}\}$ is an integral basis in $\mathbb{Q}(\alpha)$.*

• Computing discriminants. We discuss here some approaches to computing discriminants. Observe that Theorem 42 may be useful for this purpose since it gives us a method of sometimes recognizing when we have an integral basis. Some other results of computational use are as follows.

Theorem 43. *If $\beta^{(1)}, \dots, \beta^{(n)} \in \mathbb{Q}(\alpha)$, then*

$$\Delta(\beta^{(1)}, \dots, \beta^{(n)}) = det\big(Tr_{\mathbb{Q}(\alpha)}(\beta^{(i)}\beta^{(j)})\big).$$

Proof. See the proof of Theorem 40. ■

Theorem 44. *Consider the basis $1, \alpha, \dots, \alpha^{n-1}$ for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. If $f(x)$ is the minimal polynomial for α, then*

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{\mathbb{Q}(\alpha)}\big(f'(\alpha)\big).$$

Lemma. *Let $x_1, \dots, x_n$ be n variables. Then*

$$\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}^2 = (-1)^{n(n-1)/2} \prod_{\substack{1\le i\le n \\ 1\le j\le n \\ i\ne j}} (x_i - x_j).$$

Proof. It is clear that the determinant on the left-hand side is 0 if $x_i = x_j$ for any distinct i and j. This implies that the left-hand side is divisible by the product on the right. By comparing degrees, we deduce that the left-hand side is a constant, say c, times this product. An easy induction argument implies that the coefficient of $(x_2x_3^2\cdots x_n^{n-1})^2$ in the product on the right above is $(-1)^{n(n-1)/2}$. On the other hand, the coefficient of $(x_2x_3^2\cdots x_n^{n-1})^2$ in the determinant on the left is 1. It follows that $c = (-1)^{n(n-1)/2}$, and the lemma follows. ■

Proof of Theorem 44. As usual, let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ denote the conjugates of α. We have

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = \det\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{\substack{1\le i\le n \\ 1\le j\le n \\ i\ne j}} (\alpha_i - \alpha_j).$$

On the other hand,

$$f(x) = \prod_{j=1}^{n} (x - \alpha_j) \qquad \Longrightarrow \qquad f'(\alpha_i) = \prod_{\substack{1 \le j \le n \\ j \ne i}} (\alpha_i - \alpha_j)$$

for each $i \in \{1, 2, \dots, n\}$. Therefore,

$$N_{\mathbb{Q}(\alpha)}\big(f'(\alpha)\big) = f'(\alpha_1) f'(\alpha_2) \cdots f'(\alpha_n) = \prod_{\substack{1 \le i \le n \\ 1 \le j \le n \\ i \ne j}} (\alpha_i - \alpha_j).$$

The theorem follows. ■

Example: Let α be a root of $x^3 + x + 1 = 0$. Let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. We compute

$$\begin{aligned} \Delta(1, \alpha, \alpha^2) &= -N(3\alpha^2 + 1) = -(3\alpha_1^2 + 1)(3\alpha_2^2 + 1)(3\alpha_3^2 + 1) \\ &= -\big(27\alpha_1^2\alpha_2^2\alpha_3^2 + 9(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + 3(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 1\big), \end{aligned}$$

where α_1, α_2, and α_3 are the roots of $x^3 + x + 1 = 0$. We can complete our computations by using elementary symmetric functions in α_1, α_2, and α_3. Alternatively, we can use the elementary symmetric functions in α_1^2, α_2^2, and α_3^2. Observe that each α_j is a root of

$$\big((x^2 + 1)x + 1\big)\big((x^2 + 1)x - 1\big) = (x^2 + 1)^2 x^2 - 1.$$

Hence, each α_j^2 is a root of $(x + 1)^2 x - 1 = x^3 + 2x^2 + x - 1$. This gives us the elementary symmetric functions in α_1^2, α_2^2, and α_3^2. We deduce

$$\Delta(1, \alpha, \alpha^2) = -(27 \times 1 + 9 \times 1 + 3 \times (-2) + 1) = -31.$$

Since α is an algebraic integer, we obtain from Theorem 42 that $\{1, \alpha, \alpha^2\}$ is an integral basis in $\mathbb{Q}(\alpha)$. In particular, we deduce $R = \mathbb{Z}[\alpha]$ (in this case).

Cyclotomic Fields:

• Cyclotomic polynomials. Let $\zeta_n = e^{2\pi i/n}$. Since ζ_n is a root of $x^n - 1 = 0$, we deduce that ζ_n is an algebraic integer. The minimal polynomial for ζ_n we denote by $\Phi_n(x)$; it is called the nth cyclotomic polynomial. We deal with the case $n = p$ here.

• An irreducibility criterion. The following result is usually called Eisenstein's criterion for irreducibility; it was however first published by Schönemann.

Theorem 45. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$. Suppose that there exists a prime p such that $p \nmid a_n$, $p | a_j$ for all $j < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Assume that $f(x)$ is reducible over $\mathbb{Q}$. By Gauss' Lemma (Theorem 8), $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, $r = \deg g(x) > 0$, and $s = \deg h(x) > 0$. Observe that

$$g(x)h(x) \equiv f(x) \equiv a_n x^n \pmod{p}.$$

By unique factorization in $\mathbb{Z}_p[x]$ (where $\mathbb{Z}_p$ is the field of integers modulo p), we deduce that $g(x)$ and $h(x)$ are both constants times a power of x modulo p. Furthermore, the condition that $p \nmid a_n$ implies that the leading coefficient of $g(x)$ and the leading coefficient of $h(x)$ are not divisible by p. Hence, there exist integers b and c such that $g(x) \equiv bx^r \pmod{p}$ and $h(x) \equiv cx^s \pmod{p}$. Since $r > 0$ and $s > 0$, we get that p divides the constant terms of $g(x)$ and $h(x)$. This contradicts that $p^2 \nmid a_0$, completing the proof. ■

- The polynomial $\Phi_p(x)$. Using Theorem 45, we can obtain

Theorem 46. *For every prime p, $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.*

Proof. Let $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Since $\zeta_p \neq 1$ and ζ_p is a root of $x^p - 1 = (x-1)f(x)$, we obtain that ζ_p is a root of $f(x)$. Thus, it suffices to show that $f(x)$ is irreducible over $\mathbb{Q}$. Note that $f(x)$ is irreducible if and only if $f(x+1)$ is. Also,

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{j=1}^{p} \binom{p}{j} x^{j-1}$$

is irreducible by Theorem 45. Hence, $\Phi_p(x) = f(x)$. ■

Theorem 46 gives us some immediate information about ζ_p. It is easily seen that the roots of $\Phi_p(x)$ are ζ_p^j where $1 \le j \le p-1$, and hence these are the conjugates of ζ_p. We can compute norms and traces in $\mathbb{Q}(\zeta_p)$ with this information. We have $Tr(\zeta_p) = -1$ and $N(\zeta_p) = 1$ for p odd. Also,

$$Tr(1 - \zeta_p) = Tr(1) - Tr(\zeta) = p$$

and

$$N(1 - \zeta_p) = \prod_{j=1}^{p-1} (1 - \zeta_p^j) = \Phi_p(1) = p.$$

- The ring of algebraic integers in $\mathbb{Q}(\zeta_p)$.

Theorem 47. *The ring of algebraic integers in $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$.*

Proof. Let $\zeta = \zeta_p$. Let R be the ring of algebraic integers in $\mathbb{Q}(\zeta)$. Clearly, $\mathbb{Z}[\zeta] \subseteq R$. Let $\beta \in R$. Since $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ form a basis for $\mathbb{Q}(\zeta)$, there are rational numbers $a_0, a_1, \ldots, a_{p-2}$ such that $\beta = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$. It suffices to prove each a_j is in $\mathbb{Z}$. Since $\zeta^{-k} = \zeta^{p-k}$, we deduce that $\beta\zeta^{-k} - \beta\zeta$ is an algebraic integer for each

$k \in \{0, 1, \ldots, p-2\}$. By Theorem 39, the trace of $\beta\zeta^{-k} - \beta\zeta$ is in $\mathbb{Z}$. For $j \in \{1, 2, \ldots, p-1\}$, $Tr(\zeta^j) = -1$ (since ζ^j has minimal polynomial $\Phi_p(x)$). Hence,

$$\begin{aligned} Tr(\beta\zeta^{-k} - \beta\zeta) &= Tr(a_0\zeta^{-k} + \cdots + a_k + \cdots + a_{p-2}\zeta^{p-k-2} - a_0\zeta - \cdots - a_{p-2}\zeta^{p-1}) \\ &= (p-1)a_k - a_0 - \cdots - a_{k-1} - a_{k+1} - \cdots - a_{p-2} + a_0 + \cdots + a_{p-2} = pa_k. \end{aligned}$$

Hence, $pa_k \in \mathbb{Z}$ for all $k \in \{0, 1, \ldots, p-2\}$. Let $\lambda = 1 - \zeta$. Then

$$(*) \qquad p\beta = \sum_{k=0}^{p-2} (pa_k)\zeta^k = \sum_{k=0}^{p-2} (pa_k)(1-\lambda)^k = \sum_{j=0}^{p-2} c_j \lambda^j,$$

where for each $j \in \{0, 1, \ldots, p-2\}$ we have

$$c_j = \sum_{k=j}^{p-2} (-1)^j \binom{k}{j} pa_k \in \mathbb{Z}.$$

Also, since $\lambda = 1 - \zeta$, an analogous argument gives that for each $j \in \{0, 1, \ldots, p-2\}$,

$$pa_j = \sum_{k=j}^{p-2} (-1)^j \binom{k}{j} c_k.$$

It suffices therefore to prove that each c_j is divisible by p. Since

$$c_0 = \sum_{k=0}^{p-2} pa_k = p(-(p-1)a_0 + a_1 + \cdots + a_{p-2} + pa_0) = p\big(-Tr(\beta) + pa_0\big),$$

we obtain that $p | c_0$. Suppose now $p | c_j$ for $j \le k-1$. Observe that

$$p = \Phi_p(1) = \prod_{j=1}^{p-1} (1 - \zeta^j) = (1-\zeta)^{p-1} \prod_{j=1}^{p-1} (1 + \zeta + \cdots + \zeta^{j-1}) = \lambda^{p-1}\kappa,$$

where $\kappa \in \mathbb{Z}[\zeta]$ and, hence, $\kappa \in R$. From $(*)$,

$$c_k\lambda^k = p\beta - c_0 - c_1\lambda - \cdots - c_{k-1}\lambda^{k-1} - c_{k+1}\lambda^{k+1} - \cdots - c_{p-2}\lambda^{p-2}.$$

Since $p = \lambda^{p-1}\kappa$ divides each of $c_0, c_1, \ldots, c_{k-1}$, the right-hand side above can be written in the form $\lambda^{k+1}\kappa'$ for some $\kappa' \in \mathbb{Z}[\zeta] \subseteq R$. Therefore, $c_k = \lambda\kappa'$. Taking norms, we obtain

$$c_k^{p-1} = N(c_k) = N(\lambda)N(\kappa') = pN(\kappa').$$

On the other hand, Theorem 39 implies that $N(\kappa') \in \mathbb{Z}$. Hence, $p | c_k^{p-1}$, and we deduce that $p | c_k$. This completes the proof that $p | c_k$ for all $k \in \{0, 1, \ldots, p-2\}$ by induction, and the theorem follows. ■

• The discriminant of $\mathbb{Q}(\zeta_p)$ where p is an odd prime. Theorem 47 implies that $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is an integral basis in $\mathbb{Q}(\zeta_p)$. By Theorem 44, we obtain then that the discriminant is

$$\Delta = (-1)^{(p-1)(p-2)/2} N(\Phi_p'(\zeta_p)) = (-1)^{(p-1)/2} N\Big(\frac{d}{dx}\Big(\frac{x^p-1}{x-1}\Big)\Big|_{x=\zeta_p}\Big)$$

$$= (-1)^{(p-1)/2} N\Big(\frac{(x-1)px^{p-1}-(x^p-1)}{(x-1)^2}\Big|_{x=\zeta_p}\Big)$$

$$= (-1)^{(p-1)/2} N\Big(\frac{(\zeta_p-1)p\zeta_p^{p-1}-(\zeta_p^p-1)}{(\zeta_p-1)^2}\Big)$$

$$= (-1)^{(p-1)/2} N\Big(\frac{p\zeta_p^{p-1}}{\zeta_p-1}\Big) = (-1)^{(p-1)/2}\frac{p^{p-1}(-1)^{p-1}}{N(\lambda)} = (-1)^{(p-1)/2}p^{p-2},$$

where $\lambda = 1-\zeta_p$ as before. Hence, we have

Theorem 48. *The discriminant of the field $\mathbb{Q}(\zeta_p)$ is $(-1)^{(p-1)/2}p^{p-2}$.*

Units, Irreducibles, and Primes:

• A characteristic of units. Throughout the material below, α represents an algebraic number.

Theorem 49. *Let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Then $\varepsilon \in R$ is a unit in R if and only if $N_{\mathbb{Q}(\alpha)}(\varepsilon) = \pm 1$.*

Proof. Suppose ε is a unit. Then there exists $\varepsilon' \in R$ such that $\varepsilon\varepsilon' = 1$. Since ε and ε' are in R, $N(\varepsilon)$ and $N(\varepsilon')$ are in $\mathbb{Z}$. Since $N(\varepsilon)N(\varepsilon') = N(\varepsilon\varepsilon') = N(1) = 1$, it follows that $N(\varepsilon) = \pm 1$.

Now, suppose $\varepsilon \in R$ is such that $N(\varepsilon) = \pm 1$ and we want to prove ε is a unit. Let $\varepsilon_1 = \varepsilon, \varepsilon_2, \ldots, \varepsilon_n$ be the field conjugates of ε. Each ε_j being a conjugate of ε implies that each ε_j is an algebraic integer. Hence, $\varepsilon' = \varepsilon_2\varepsilon_3\cdots\varepsilon_n$ is an algebraic integer. Also, $\pm 1 = N(\varepsilon) = \varepsilon\varepsilon'$ implies $\varepsilon' = \pm 1/\varepsilon \in \mathbb{Q}(\alpha)$. Therefore, $\varepsilon' \in R$ and $\varepsilon\varepsilon' = \pm 1$. It follows that ε is a unit. ■

• Definitions. Let β and γ be in R (where R is the ring of algebraic integers in $\mathbb{Q}(\alpha)$). We write $\gamma|\beta$ and say γ *divides* β if there is a $\delta \in R$ such that $\beta = \gamma\delta$. Suppose $\beta \in R - \{0\}$ and β is not a unit. If $\beta = \gamma\delta$ with γ and δ in R implies that either γ or δ is a unit in R, then β is *irreducible*. If $\beta|\gamma\delta$ implies that either $\beta|\gamma$ or $\beta|\delta$, then β is *prime*. Note that all primes are irreducibles.

• Existence of factorizations.

Theorem 50. *Every nonunit element in $R - \{0\}$, where R is the ring of algebraic integers in $\mathbb{Q}(\alpha)$, can be written as a finite product of irreducibles in R.*

Proof. Let $\beta \in R - \{0\}$ with β not a unit. By Theorem 49, $|N(\beta)| > 1$. If β is irreducible, then we're through. Otherwise, there exist γ and δ in R with γ and δ nonunits such that $\beta = \gamma\delta$. Then $N(\beta) = N(\gamma)N(\delta)$ and $|N(\gamma)| > 1$ and $|N(\delta)| > 1$ so that $1 < |N(\gamma)| < |N(\beta)|$ and $1 < |N(\delta)| < |N(\beta)|$. By Theorem 39, $|N(\beta)|$, $|N(\gamma)|$, and $|N(\delta)|$ are in $\mathbb{Z}$. If γ or δ is not irreducible, we may repeat the above procedure to obtain numbers in R with smaller norms in absolute value. The procedure may be repeated again and again but must eventually end resulting in a factorization of β into irreducibles. ■

The factorization in Theorem 50 may not be unique. For example,

$$21 = 3 \times 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

in the ring R of algebraic integers in $\mathbb{Q}(\sqrt{-5})$. We show that each of 3, 7, $4 + \sqrt{-5}$, and $4 - \sqrt{-5}$ is irreducible in R. Since $-5 \equiv 3 \pmod 4$, we get from Theorem 10 that $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Assume

$$3 = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$$

is a factorization of 3 into nonunits in R. Then taking norms, we obtain $9 = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$ so that $a_1^2 + 5b_1^2 = 3$ and $a_2^2 + 5b_2^2 = 3$. But $x^2 + 5y^2 = 3$ has no solutions in integers, giving a contradiction. Therefore, 3 is irreducible in R. A similar argument shows that 7 is irreducible. Now, assume

$$4 \pm \sqrt{-5} = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$$

is a factorization of $4 \pm \sqrt{-5}$ into nonunits in R. Upon taking norms, we deduce that one of $a_1^2 + 5b_1^2$ and $a_2^2 + 5b_2^2$ is 3 and the other is 7. Since $x^2 + 5y^2 = 3$ (and $x^2 + 5y^2 = 7$) has no solutions in integers, we obtain a contradiction. Hence, each of $4 + \sqrt{-5}$ and $4 - \sqrt{-5}$ is irreducible. Thus, 21 does not factor uniquely into irreducibles in R.

- A property of primes. Here, we prove

Theorem 51. *Let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$, and let β be a prime in R. Then there is a unique prime p in $\mathbb{Z}$ (a rational prime) such that $\beta|p$ in R.*

Proof. Let $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be the field polynomial for β. Then $a_0 = \pm N(\beta)$ and $F(\beta) = 0$ imply

$$\beta(\beta^{n-1} + a_{n-1}\beta^{n-2} + \cdots + a_1) = -a_0 = \mp N(\beta).$$

Hence, $\beta|N(\beta)$ in R. Since $N(\beta) \in \mathbb{Z}$, there is a minimal positive integer $k \in \mathbb{Z}$ such that $\beta|k$ in R. We prove k is a rational prime. Observe that $k \neq 1$ since $\beta|1$ would imply β is a unit, contradicting that β is prime. Assume $k = k_1k_2$ with k_1 and k_2 rational integers > 1. Then $\beta|k_1k_2$ implies that $\beta|k_1$ and $\beta|k_2$, contradicting the minimality of k. Hence, k is prime.

Suppose now that $\beta|p$ and $\beta|q$ in R where p and q are distinct rational primes. Then using that there exist rational integers x and y such that $px + qy = 1$, we deduce that $\beta|1$, a contradiction. Hence, there is a unique rational prime p such that $\beta|p$ in R. ■

Homework: For the following problems, take R to be the ring of algebraic integers in an algebraic number field $\mathbb{Q}(\alpha)$.

(1) Prove that if u is a unit in R and β is an irreducible element of R, then $u\beta$ is irreducible.

(2) Prove that all primes in R are irreducible.

(3) Prove that 6 cannot be factored as a product of primes in the ring of algebraic integers in $\mathbb{Q}(\sqrt{-5})$.

(4) Let $\beta \in R$. Prove that if $N(\beta)$ is a rational prime, then β is irreducible in R.

Euclidean Domains, PID's, and UFD's:

• Definitions. Let $\mathbb{Q}(\alpha)$ be an algebraic number field and R its ring of algebraic integers. The results in this section will, however, hold in the more general situation of R being a domain (a commutative ring with a non-zero multiplicative identity and having no zero divisors). We say that *R is a Euclidean domain* if there exists a function $\phi : R - \{0\} \mapsto \mathbb{Z}^+$ such that (i) if β and γ are in $R - \{0\}$ and $\beta|\gamma$ in R, then $\phi(\beta) \le \phi(\gamma)$; and (ii) if β and γ are in $R - \{0\}$, then there are q and r in R such that $\beta = \gamma q + r$ with either $r = 0$ or $\phi(r) < \phi(\gamma)$. We say that *R is a principal ideal domain (or a PID)* if every ideal in R is principal. We say that *R is a unique factorization domain (or a UFD)* if every $\beta \in R$ has the property that whenever $\beta = up_1p_2\cdots p_r = vq_1q_2\cdots q_s$ where u and v are units in R and $p_1, p_2, \dots, p_r$ and $q_1, q_2, \dots, q_s$ are irreducibles in R, we have $r = s$ and by appropriately rearranging subscripts, one gets that $p_j = u_jq_j$ for $j \in \{1, 2, \dots, r\}$ and some units u_j.

• A theorem connecting irreducibles and primes in UFD's.

Theorem 52. *Every irreducible is prime in R if and only if R is a UFD.*

Proof. Suppose first that R is a UFD. Let p be an irreducible, and suppose $p|\beta\gamma$ in R (so β and γ are in R). We want to show that $p|\beta$ or $p|\gamma$. It suffices to consider $\beta\gamma \ne 0$. Let $\delta \in R$ be such that $p\delta = \beta\gamma$. Write

$$\beta = up_1p_2\cdots p_r, \quad \gamma = vq_1q_2\cdots q_s, \quad \text{and} \quad \delta = w\ell_1\ell_2\cdots\ell_t,$$

where u, v, and w are units and $p_1, \dots, p_r$, $q_1, \dots, q_s$, and $\ell_1, \dots, \ell_t$ are irreducibles in R. Then

$$pw\ell_1\ell_2\cdots\ell_t = uvp_1p_2\cdots p_rq_1q_2\cdots q_s.$$

Note that any divisor of a unit is a unit. Since R is a UFD, it follows that p divides some p_j (and, hence, β) or p divides some q_j (and, hence, γ). This implies that p is a prime.

Now, suppose every irreducible in R is prime, and we want to show that R is a UFD. Consider

$$(*) \qquad up_1p_2\cdots p_r = vq_1q_2\cdots q_s,$$

where u and v are units and $p_1, \dots, p_r$ and $q_1, \dots, q_s$ are irreducibles (and, hence, primes) in R. Let $j \in \{1, 2, \dots, r\}$. Since p_j is prime, $p_j|q_i$ for some $i \in \{1, 2, \dots, s\}$. Write

$q_i = \beta_j p_j$ where $\beta_j \in R$. Since q_i is irreducible and p_j is a nonunit, we deduce that β_j is a unit. Multiplying through by β_j in $(*)$ and cancelling $\beta_j p_j$ with q_i, the number of prime factors on each side of $(*)$ decreases by one. Continuing in this manner, we get that $r = s$ and (after rearranging) $q_j = \beta_j p_j$ for each $j \in \{1, 2, \dots, r\}$ with β_j a unit in R. This implies that R is a UFD. ■

- Some implications.

Theorem 53. *If R is a Euclidean domain, then R is a PID.*

Proof. Let I be an ideal in R. We may suppose there is a $\beta \in I$ such that $\beta \neq 0$. Take such a β with $\phi(\beta)$ as small as possible. Let $\gamma \in I$. Write $\gamma = \beta q + r$ where q and r are in R with either $r = 0$ or $\phi(r) < \phi(\beta)$. But $r = \gamma - \beta q \in I$ implies $r = 0$. Hence, $\gamma = \beta q$. It follows that $I \subseteq (\beta) \subseteq I$ so that $I = (\beta)$, completing the proof. ■

Theorem 54. *If R is a PID, then R is a UFD.*

Proof. Let p be an irreducible element of R. By Theorem 52, it suffices to show that p must be prime. Suppose $p|\beta\gamma$ where β and γ are in R. Also, suppose $p \nmid \beta$ in R. Since R is a PID, there is a δ such that $(p, \beta) = (\delta)$. It follows that $p = \delta\delta'$ and $\beta = \delta\delta''$ for some δ' and δ'' in R. Observe that δ' is not a unit since otherwise we would have $\beta = \delta\delta'' = p(\delta')^{-1}\delta''$, contradicting that $p \nmid \beta$. Since p is irreducible and $p = \delta\delta'$, we obtain that δ is a unit. This implies that $1 \in (\delta)$. Since $(p, \beta) = (\delta)$, there exist λ and λ' in R such that $p\lambda + \beta\lambda' = 1$. Multiplying by γ, we obtain

$$\gamma = p\Big(\gamma\lambda + \frac{\beta\gamma}{p}\lambda'\Big).$$

Since $\beta\gamma/p \in R$, we deduce that $p|\gamma$. This implies that p is a prime. ■

Theorem 55. *If R is a Euclidean domain, then R is a UFD.*

Proof. This follows from the previous two theorems. ■

More on Quadratic Extensions:

- Some Euclidean domains. We describe some examples of Euclidean domains. Keep in mind that Theorems 53 and 55 imply that such domains are PID's and UFD's.

Theorem 56. *Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. Then R is a Euclidean domain for $N = -1$, -2, -3, -7, and -11.*

Proof. We show that we can take $\phi(\beta)$ in the definition of a Euclidean domain to be $|N_{\mathbb{Q}(\sqrt{N})}(\beta)|$. Let β and γ be in $R - \{0\}$. If $\beta|\gamma$, then $N(\beta)$ and $N(\gamma)$ are rational integers with $N(\beta)|N(\gamma)$. It easily follows that $\phi(\beta) = |N(\beta)| \leq |N(\gamma)| = \phi(\gamma)$. Considering now more general β and γ be in $R - \{0\}$, we show that there are q and r in R such that $\beta = q\gamma + r$ and either $r = 0$ or $\phi(r) < \phi(\gamma)$. Define $\delta = \beta/\gamma \in \mathbb{Q}(\sqrt{N})$. We need only show that there is a $q \in R$ for which $|N(\delta - q)| < 1$. Write $\delta = u + v\sqrt{N}$ where u and v are rational. If $N \not\equiv 1 \pmod 4$ (so N is -1 or -2), then we want x and y in $\mathbb{Z}$ for which

$$|N(\delta - (x + y\sqrt{N}))| = |N((u - x) + (v - y)\sqrt{N})| = (u - x)^2 - N(v - y)^2 < 1.$$

We take x to be the nearest integer to u and y to be the nearest integer to v. Then $(u-x)^2 - N(v-y)^2 < (1/4) + 2(1/4) < 1$. If $N \equiv 1 \pmod 4$, then $R = \mathbb{Z}[(1+\sqrt{N})/2]$ and we want x and y in $\mathbb{Z}$ for which

$$\left|N\Big(\delta - \Big(x + y\frac{1+\sqrt{N}}{2}\Big)\Big)\right| = \left|N\Big(\Big(u-x-\frac{y}{2}\Big)+\Big(v-\frac{y}{2}\Big)\sqrt{N}\Big)\right| = \Big(u-x-\frac{y}{2}\Big)^2 - N\Big(v-\frac{y}{2}\Big)^2 < 1.$$

Take $y \in \mathbb{Z}$ such that $|v-(y/2)| \le 1/4$ and then take $x \in \mathbb{Z}$ so that $|u-x-(y/2)| \le 1/2$. Then

$$\Big(u-x-\frac{y}{2}\Big)^2 - N\Big(v-\frac{y}{2}\Big)^2 \le \frac{1}{4} + \frac{11}{16} < 1.$$

This completes the proof. ■

Recall that we showed that there is not unique factorization in the ring R of algebraic integers in $\mathbb{Q}(\sqrt{-5})$. Thus, R is is not a Euclidean domain by Theorem 52. The exact values of N for which the ring R of algebraic integers in $\mathbb{Q}(\sqrt{N})$ is Euclidean is unknown. We state the following without proof.

Theorem 57. *Let N be squarefree, and let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. For $N < 0$, R is Euclidean if and only if $N = -1$, -2, -3, -7, or -11. For $N > 0$, R is Euclidean with the Euclidean function $\phi(\beta) = |N(\beta)|$ if and only if $N = 2$, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, or 73.*

Open Problem 1. Is there a positive integer $N \ne 69$ such that the ring R is Euclidean and N is not in the list above?

Open Problem 2. Do there exist infinitely many positive integers N for which the ring R is a UFD?

Comment: For $N = 14$ it is known that R is a UFD and that it is not Euclidean with Euclidean function $\phi(\beta) = |N(\beta)|$. However, it is unknown whether R is Euclidean.

- Units in imaginary quadratic extensions. We have already discussed units in the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$ when $N > 0$. Here we summarize the situation for $N < 0$ with the following:

Theorem 58. *Let N be a negative integer with N squarefree. Let U be the units in R, the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. Then*

(i) for $N = -1$, $U = \{1, -1, i, -i\}$,

(ii) for $N = -3$, $U = \{1, -1, e^{2\pi i/3}, -e^{2\pi i/3}, e^{4\pi i/3}, -e^{4\pi i/3}\}$, and

(iii) for all other N as above, $U = \{1, -1\}$.

Proof. Let $\beta = a + b\sqrt{N} \in U$ with a and b in $\mathbb{Q}$. By Theorem 49, $N(\beta) = a^2 - Nb^2 = \pm 1$. If $N = -1$, then a and b are in $\mathbb{Z}$ and it follows that (a, b) is $(\pm 1, 0)$ or $(0, \pm 1)$ so that (i) holds. If $N \not\equiv 1 \pmod 4$ and $N < -1$, then a and b are in $\mathbb{Z}$ and $a^2 - Nb^2 = 1$; hence, (iii) follows in the case $N \not\equiv 1 \pmod 4$. If $N = -3$, then $a = x/2$ and $b = y/2$ for some rational integers x and y. Since $a^2 - Nb^2 = \pm 1$, we obtain $x^2 - Ny^2 = \pm 4$ so that (x, y) is $(\pm 2, 0)$, $(\pm 1, 1)$, or $(\pm 1, -1)$. Since $e^{2\pi i/3} = (-1 + \sqrt{-3})/2$ and $e^{4\pi i/3} = (-1 - \sqrt{-3})/2$, we obtain (ii). If $N \equiv 1 \pmod 4$ and $N < -3$, then $a = x/2$ and $b = y/2$ for some rational integers x and y satisfying $x^2 - Ny^2 = 4$ so that $(x, y) = (\pm 2, 0)$. Hence, (iii) holds, completing the proof of the theorem. ■

Applications:

- When is a prime a sum of two squares?

Theorem 59. *Let p be a rational prime. Then p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Furthermore, if p is a sum of two squares, then the squares are uniquely determined.*

Lemma. *If $p \equiv 1 \pmod 4$, then there is an $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \pmod p$.*

Proof 1. By unique factorization modulo p and the congruence

$$(x^{(p-1)/2} + 1)(x^{(p-1)/2} - 1) = (x-1)(x-2)\cdots(x-(p-1)) \pmod p,$$

we deduce that there is a $b \in \{1, 2, \dots, p-1\}$ for which $b^{(p-1)/2} + 1 \equiv 0 \pmod p$. Take $a = b^{(p-1)/4}$. ■

Proof 2. If $x \in \{2, 3, \dots, p-2\}$ and $y \in \mathbb{Z}$ with $xy \equiv 1 \pmod p$, then y is not congruent to 0, 1, -1, or x modulo p. Pair the numbers in $\{2, 3, \dots, p-2\}$ so that each pair (x, y) satisfies $xy \equiv 1 \pmod p$. We deduce $\prod_{j=2}^{p-2} j \equiv 1 \pmod p$. Hence, $(p-1)! \equiv -1 \pmod p$. But

$$\begin{aligned}(p-1)! &\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \times \cdots \times (-2) \times (-1) \\ &\equiv (-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p.\end{aligned}$$

Take $a = ((p-1)/2)!$. ■

Proof of Theorem 59. Clearly the theorem holds for $p = 2$. For any integers x and y, it is easy to check that $x^2 + y^2 \not\equiv 3 \pmod 4$. Thus, every prime (or number) $p \equiv 3 \pmod 4$ cannot be the sum of two squares. It remains to show that every prime $p \equiv 1 \pmod 4$ has a unique representation as a sum of two squares. Fix a prime $p \equiv 1 \pmod 4$, and let a be an integer as in the lemma. We consider $R = \mathbb{Z}[i]$, the ring of algebraic integers in $\mathbb{Q}(i)$. By Theorem 56, R is Euclidean. By Theorem 55, R is a UFD. By Theorem 52 (and homework), primes and irreducibles are the same in R. Assume p is prime in R. By the definition of a, we have $p|(a+i)(a-i)$ so that $p|(a+i)$ or $p|(a-i)$. But this implies that $(a+i)/p$ or $(a-i)/p$ is in $\mathbb{Z}[i]$ which is impossible. Therefore, p is not prime in R. Hence, p is not irreducible in R. Thus, there exist non-units β and γ in R such that $p = \beta\gamma$. Since $p^2 = N(p) = N(\beta)N(\gamma)$ and $N(\beta)$ and $N(\gamma)$ are integers > 1, we must have that each of $N(\beta)$ and $N(\gamma)$ is p. Taking $\beta = x + iy$ where x and y are rational integers, we obtain $p = N(\beta) = x^2 + y^2$. This proves that p is a sum of two squares. If x_0 and y_0 are also rational integers with $p = x_0^2 + y_0^2$, then $(x_0 + iy_0)(x_0 - iy_0) = (x + iy)(x - iy)$. By a previous homework assignment, the norm of each of these four factors being a rational prime implies they are each irreducible. By Theorem 58, the units in R are just ± 1 and $\pm i$. Since R is a UFD, we deduce that $x_0 + iy_0$ is $\epsilon(x \pm iy)$ for some ϵ in $\{1, -1, i, -i\}$. In any case, $\{x_0^2, y_0^2\} = \{x^2, y^2\}$, and the theorem follows. ■

- When can a positive integer be written as a sum of two squares?

Theorem 60. *Let n be a positive integer. Write n in the form*

$$n = 2^t \prod_{j=1}^{r} p_j^{e_j} \prod_{j=1}^{s} q_j^{f_j}$$

where t, r, s, the e_j's, and the f_j's are nonnegative integers, the p_j's and the q_j's are distinct primes, $p_j \equiv 1 \pmod 4$ for each $j \in \{1, 2, \ldots, r\}$, and $q_j \equiv 3 \pmod 4$ for each $j \in \{1, 2, \ldots, s\}$. Then n can be written as a sum of two squares if and only if each f_j is even.

Proof. Suppose that $n = x^2 + y^2$ for some integers x and y and that there is a prime $q \equiv 3 \pmod 4$ dividing n. Let f be maximal such that $q^f | n$. Since q cannot be written as a sum of two squares (by Theorem 59), q is irreducible and, therefore, prime in $\mathbb{Z}[i]$. Assume $f = 2g + 1$ for some integer g. Then since $\mathbb{Z}[i]$ is a UFD and $q^f | (x + iy)(x - iy)$, we obtain that either $q^{g+1} | (x + iy)$ or $q^{g+1} | (x - iy)$. Taking norms gives that $q^{g+2} = q^{f+1}$ divides n, giving a contradiction. Hence, each f_j is even.

Now, supppose we are given n with each f_j even. Then $q_j^{f_j} = 0^2 + (q_j^{f_j/2})^2$ and Theorem 59 imply that each of $2, p_1, \ldots, p_r, q_1^{f_1}, \ldots, q_s^{f_s}$ can be expressed as a sum of two squares. It suffices, therefore, to prove that for any integers x_1, y_1, x_2, and y_2, there exist integers x_3 and y_3 satisfying

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x_3^2 + y_3^2.$$

This easily follows by setting $x_3 + iy_3 = (x_1 + iy_1)(x_2 + iy_2)$ and taking norms. ■

Homework:

(1) Suppose n is a positive integer expressed in the form given in Theorem 60 with each f_j even. Let $r(n)$ denote the number of pairs (x, y) with x and y in $\mathbb{Z}$ and $n = x^2 + y^2$. Find a formula for $r(n)$ that depends only on t and r.

(2) Determine the primes $p > 3$ which can be expressed in the form $a^2 + 3b^2$ for some integers a and b. For example, 7 is such a prime since $7 = 2^2 + 3 \times 1^2$. Your final answer should be written as "$p = a^2 + 3b^2$ for some integers a and b if and only if $p \equiv L \pmod N$" where N is some positive integer and where L is a list of congruence classes modulo N. (You may use information about quadratic residues modulo primes.)

- We have discussed how to solve $x^2 - Ny^2 = B$ when $|B| \le \sqrt{N}$ (see Theorem 30). Here, we give an example of a slightly different situation.

Theorem 61. *The solutions of $x^2 - 29y^2 = 35$ in integers x and y are given by*

$$x + y\sqrt{29} = \pm(8+\sqrt{29})(70+13\sqrt{29})^k, \quad x + y\sqrt{29} = \pm(8-\sqrt{29})(70+13\sqrt{29})^k,$$

$$x+y\sqrt{29} = \pm(124+23\sqrt{29})(70+13\sqrt{29})^k, \text{ and } x+y\sqrt{29} = \pm(124-23\sqrt{29})(70+13\sqrt{29})^k,$$

where $k \in \mathbb{Z}$.

Proof. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{29})$. By Theorems 57 and 55, R is a UFD. By Theorem 52, irreducibles and primes (and homework) are the same in R. Using $\sqrt{29} = [5, \overline{2,1,1,2,10}]$, one gets that $5 = (11+2\sqrt{29})(11-2\sqrt{29})$, $7 = (6+\sqrt{29})(6-\sqrt{29})$, and $\epsilon = (5+\sqrt{29})/2$ is the fundamental unit in R. Since the norms of $11 \pm 2\sqrt{29}$ and $6 \pm \sqrt{29}$ are rational primes, they are irreducible and hence prime in R. If $x^2 - 29y^2 = 35$, then

$$(x+y\sqrt{29})(x-y\sqrt{29}) = (11+2\sqrt{29})(11-2\sqrt{29})(6+\sqrt{29})(6-\sqrt{29}).$$

Note that $11+2\sqrt{29}$ and $11-2\sqrt{29}$ cannot both divide $x+y\sqrt{29}$; otherwise, $5|x$ and $5|y$ in R so that $25|(x+y\sqrt{29})(x-y\sqrt{29})$ in R which implies $25|35$ in R which is impossible. Similarly, $11+2\sqrt{29}$ and $11-2\sqrt{29}$ cannot both divide $x-y\sqrt{29}$, and also $6+\sqrt{29}$ and $6-\sqrt{29}$ cannot both divide one of $x+y\sqrt{29}$ and $x-y\sqrt{29}$. Since $(11 \pm 2\sqrt{29})(6 \pm \sqrt{29}) = 124 \pm 23\sqrt{29}$ and $(11 \pm 2\sqrt{29})(6 \mp \sqrt{29}) = 8 \pm \sqrt{29}$, we get that $x + y\sqrt{29}$ is one of $\pm(8+\sqrt{29})\epsilon^k$, $\pm(8-\sqrt{29})\epsilon^k$, $\pm(11+2\sqrt{29})\epsilon^k$, and $\pm(11-2\sqrt{29})\epsilon^k$ for some integer k. Suppose for the moment that $\epsilon^k \notin \mathbb{Z}[\sqrt{29}]$ (note that $R = \mathbb{Z}[(1+\sqrt{29})/2]$). Then $\epsilon^k = (a+b\sqrt{29})/2$ where a and b are odd. But then $x+y\sqrt{29}$, being of one of the above forms, is not in $\mathbb{Z}[\sqrt{29}]$. More precisely, x and y are not in $\mathbb{Z}$, which is a contradiction. Hence, we must have $\epsilon^k = a+b\sqrt{29} \in \mathbb{Z}[\sqrt{29}]$. It is clear now that any such $x+y\sqrt{29}$ gives rise to a solution to $x^2 - 29y^2 = 35$. Observe that $\epsilon^k = a + b\sqrt{29}$ implies $a^2 - 29b^2 = \pm 1$. The result now follows from Theorem 32, Theorem 33, and $\sqrt{29} = [5, \overline{2,1,1,2,10}]$. ■

- An elementary argument. Before giving our next application of algebraic techniques, we illustrate an elementary argument for a similar result.

Theorem 62. *The equation $y^2 + 5 = x^3$ has no solutions in integers x and y.*

Lemma. *If p is a prime with $p \equiv 3 \pmod 4$, then there does not exist an integer a such that $a^2 \equiv -1 \pmod p$.*

Proof. Assume $a^2 \equiv -1 \pmod p$ holds for some integer a. Since $(p-1)/2$ is odd,

$$a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv -1 \pmod p.$$

Fermat's Little Theorem implies a^{p-1} is either 0 or 1 modulo p, giving a contradiction. Hence, the lemma follows. ■

Proof of Theorem 62. Assume there are integers x and y satisfying $y^2 + 5 = x^3$. Then $y^2 \equiv x^3 - 1 \pmod 4$ implies that $x \equiv 1 \pmod 4$ (anything else leads to a contradiction). Observe that

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2+x+1)$$

and $x^2+x+1 \equiv 3 \pmod 4$. It follows that there must be a prime $p \equiv 3 \pmod 4$ dividing x^2+x+1 and, hence, y^2+4. But $p|(y^2+4)$ implies that $(y \times 2^{-1})^2 \equiv -1 \pmod p$, a contradiction to the lemma. This establishes the theorem. ■

- The equation $y^2+4=x^3$. This equation is similar to the one which appeared in Theorem 62, but there is one big difference. This equation has integer solutions.

Theorem 63. *The equation $y^2+4=x^3$ has only the rational integer solutions $(x,y) = (2,\pm 2)$ and $(5,\pm 11)$.*

Proof. Clearly $(x,y) = (2,\pm 2)$ and $(5,\pm 11)$ all are solutions of $y^2+4=x^3$, and so it remains to show that these are the only solutions in rational integers. Suppose x and y are in $\mathbb{Z}$ and satisfy $y^2+4=x^3$. We consider two cases.

Case 1. y is odd.

We work in $\mathbb{Z}[i]$. We have

$$(*) \qquad (2+iy)(2-iy) = x^3.$$

Let $a+bi$ be a common factor of $2+iy$ and $2-iy$. Since $4 = (2+iy)+(2-iy)$, we deduce that $(a+bi)|4$. Using also that $(a+bi)|(2+iy)$ and taking norms, we obtain that a^2+b^2 divides both 16 and $4+y^2$. But in this case, $4+y^2$ is odd, so $a^2+b^2=1$. This implies that $a+bi$ is a unit in $\mathbb{Z}[i]$. By writing the right-hand side of $(*)$ as a product of irreducibles, it follows from unique factorization in $\mathbb{Z}[i]$ that $2+iy = \epsilon(a+bi)^3$ for some a and b in $\mathbb{Z}$ and $\epsilon \in \{1,-1,i,-i\}$. Note that ϵ is a cube in $\mathbb{Z}[i]$ since $1^3=1$, $(-1)^3=-1$, $(-i)^3=i$, and $i^3=-i$. Hence, there are c and d in $\mathbb{Z}$ such that $2+iy=(c+di)^3$. Comparing real parts, we obtain $2 = c^3-3cd^2 = c(c^2-3d^2)$. This implies $c=\pm 1$ or $c = \pm 2$ which in turn implies (c,d) is $(-1,\pm 1)$ or $(2,\pm 1)$. Therefore,

$$x^3 = (2+iy)(2-iy) = (c+di)^3(c-di)^3 = (c^2+d^2)^3$$

is either 2^3 or 5^3. Since y is odd and $y^2+4=x^3$, we get the only solutions in this case are $(x,y) = (5,\pm 11)$.

Case 2. y is even.

Here $y=2y'$ for some integer y'. Since $y^2+4=x^3$, we obtain $x=2x'$ for some integer x'. Hence, $(y')^2+1 = 2(x')^3$. This implies that y' is odd. Write $y'=2k+1$ where $k \in \mathbb{Z}$. We work again in $\mathbb{Z}[i]$. Suppose $a+bi \in \mathbb{Z}[i]$ is a common factor of $y'+i$ and $y'-i$. Then $(a+bi)|(2i)$. Observe that $2i = (1+i)^2$ and $1+i$ is irreducible in $\mathbb{Z}[i]$ since its norm is a rational prime. Thus, by unique factorization in $\mathbb{Z}[i]$, we deduce that, for some unit ϵ in $\mathbb{Z}[i]$, either $a+bi=\epsilon$, $a+bi = \epsilon(1+i)$, or $a+bi=\epsilon(1+i)^2$. Since y' is odd, $(y')^2+1 \equiv 2 \pmod 4$ so that $4 \nmid ((y')^2+1)$. Using norms, it follows that $\epsilon(1+i)^2$ cannot divide $y' \pm i$. This shows that the only possible common prime divisor of $y'+i$ and $y'-i$ is $1+i$, and it divides each of $y'+i$ and $y'-i$ at most once. In fact, $1+i$ divides each of $y'+i$ and $y'-i$ since $y'=2k+1$ implies $y'+i = (2k+1)+i = (1+i)(k+1-ki)$ and $y'-i = (2k+1)-i = (1+i)(k-(k+1)i)$. Recall (from Case 1) that units are cubes in $\mathbb{Z}[i]$. The equation

$$(y'+i)(y'-i) = 2(x')^3 = (1+i)(1-i)(x')^3 = (1+i)^2(ix')^3$$

now implies by unique factorization in $\mathbb{Z}[i]$ that $y' + i = (1+i)(c+di)^3$ for some c and d in $\mathbb{Z}$. Comparing imaginary parts of the equation $y' + i = (1+i)(c+di)^3$ gives

$$1 = c^3 - 3cd^2 + 3c^2d - d^3 = (c-d)(c^2 + 4cd + d^2).$$

Since $(c^2 + 4cd + d^2)|1$, either one of c or d is zero or they are of opposite signs. Then $(c-d)|1$ implies one c or d is zero. It follows that $c^2+4cd+d^2 = 1$ and, hence, $c - d = 1$. Thus, (c, d) is either $(1, 0)$ or $(0, -1)$. Since

$$2(x')^3 = (y')^2 + 1 = (y' + i)(y' - i) = (1+i)(c+di)^3(1-i)(c-di)^3 = 2(c^2+d^2)^3 = 2,$$

we deduce that $x' = 1$ and, hence, $x = 2x' = 2$ and $y = \pm 2$.

Combining the two cases, the proof is complete. ■

Homework:

(1) Prove that the only integer solutions to $y^2 + 2 = x^3$ are $(x, y) = (3, \pm 5)$. (Hint: Consider two cases as in the proof above. Use arithmetic in $\mathbb{Z}[\sqrt{-2}]$. Be clear about what Theorems you are using.)

(2) Consider all the pairs of integers satisfying $y^2 + 11 = x^3$.

(a) Prove that there are no solutions with y odd.

(b) Prove that there are ≤ 100 pairs of integers (x, y) with $y^2 + 11 = x^3$.

• A conjecture of Ramanujan. The next result was conjectured by Ramanujan and first verified by Nagell.

Theorem 64. *The only solutions of the equation*

$$x^2 + 7 = 2^n$$

where x and n are in $\mathbb{Z}$ are given by $x = \pm 1$, ± 3, ± 5, ± 11, and ± 181 and $n = 3$, 4, 5, 7, and 15, respectively.

Proof. One checks that the values of x and n indicated in the theorem are in fact solutions to $x^2+7 = 2^n$. To show that these are the only solutions, it suffices to only consider $x > 0$ and $n > 3$, and we do so. We fix such a solution to $x^2+7 = 2^n$. Clearly, x is odd. We work in $\mathbb{Q}(\sqrt{-7})$. More specifically, we work in the ring $R = \mathbb{Z}[(1+\sqrt{-7})/2]$. By Theorems 55 and 56, R is a UFD. Also, by Theorem 52 (and homework), irreducibles and primes are the same in R. We consider two cases.

Case 1. n is even.

From $(2^{n/2} + x)(2^{n/2} - x) = 7$ and $2^{n/2} + x > 2^{n/2} - x$, we obtain that $2^{n/2} + x = 7$ and $2^{n/2} - x = 1$. This implies that $2^{(n/2)+1} = 8$ so that $n = 4$ and $x = 3$.

Case 2. n is odd.

Let $m = n - 2 \geq 2$. Then

$$\Big(\frac{x+\sqrt{-7}}{2}\Big)\Big(\frac{x-\sqrt{-7}}{2}\Big) = \frac{x^2+7}{4} = 2^m = \Big(\frac{1+\sqrt{-7}}{2}\Big)^m\Big(\frac{1-\sqrt{-7}}{2}\Big)^m.$$

Since the norms of $(1+\sqrt{-7})/2$ and $(1-\sqrt{-7})/2$ are rational primes, each of $(1+\sqrt{-7})/2$ and $(1-\sqrt{-7})/2$ is irreducible in R. Neither $(1+\sqrt{-7})/2$ nor $(1-\sqrt{-7})/2$ divides both of $(x+\sqrt{-7})/2$ and $(x-\sqrt{-7})/2$ since otherwise it would divide the difference $\sqrt{-7}$, which is impossible (to see this use norms). By Theorem 58, the only units in R are ± 1. By unique factorization, we deduce that

$$(*) \qquad \frac{x+\sqrt{-7}}{2} = \pm\Big(\frac{1+\epsilon\sqrt{-7}}{2}\Big)^m \quad \text{and} \quad \frac{x-\sqrt{-7}}{2} = \pm\Big(\frac{1-\epsilon\sqrt{-7}}{2}\Big)^m,$$

where $\epsilon \in \{1,-1\}$ and where the same signs occur in front of both expressions on the right. We claim

$$(**) \qquad -\sqrt{-7} = \Big(\frac{1+\sqrt{-7}}{2}\Big)^m - \Big(\frac{1-\sqrt{-7}}{2}\Big)^m.$$

Using $(*)$ and subtracting, we obtain that $(**)$ is true with the left-hand side replaced by $\pm\sqrt{-7}$. Let $\alpha = (1+\sqrt{-7})/2$ and $\beta = (1-\sqrt{-7})/2$. We have that α and β are primes in R and $\alpha\beta = 2$. Since β is prime, we know β is not a unit and, hence, $\beta \nmid 1$. Observe that

$$\alpha^2 = (1-\beta)^2 = 1 - 2\beta + \beta^2 = 1 - \alpha\beta^2 + \beta^2 = 1 + \beta^2(1-\alpha) = 1 + \beta^3.$$

Therefore,

$$\alpha^m - \alpha = \alpha(\alpha^2)^{(m-1)/2} - \alpha = \alpha(1+\beta^3)^{(m-1)/2} - \alpha = \beta^3\gamma,$$

for some $\gamma \in R$. Assume $(**)$ holds with the left-hand side replaced by $\sqrt{-7}$. Then $\alpha - \beta = \sqrt{-7} = \alpha^m - \beta^m$ so that $\beta^m - \beta = \alpha^m - \alpha = \beta^3\gamma$. This implies $\beta^{m-1} - 1 = \beta^2\gamma$ and, hence, $\beta | 1$, a contradiction. Thus, $(**)$ must hold.

From $(**)$, we obtain

$$-2^m\sqrt{-7} = (1+\sqrt{-7})^m - (1-\sqrt{-7})^m$$

so that

$$-2^m = 2\Big(\binom{m}{1} - 7\binom{m}{3} + 7^2\binom{m}{5} - \cdots\Big).$$

It follows that $2^{m-1} \equiv -m \pmod 7$. Using that $2^3 \equiv 1 \pmod 7$, we obtain

$$m \equiv 3, 5, \text{ or } 13 \pmod{21}$$

(for example, if $m \equiv 6 \pmod 7$, then $2^{m-1} \equiv -6 \equiv 1 \pmod 7$ so that $m \equiv 1 \pmod 3$ which implies $m \equiv 13 \pmod{21}$). Now, $m = 3$, 5, and 13 give us the solutions with $n = m + 2 = 5$, 7, and 15. It remains to prove that these are the only m giving rise to a solution.

Assume that m' gives rise to another solution with n odd and $n > 3$. Let $m \in \{3, 5, 13\}$ with $m' \equiv m \pmod{21}$. Note that $(**)$ holds as is and also with m replaced by m'. Let ℓ be the positive integer satisfying $7^\ell \| (m' - m)$. We will obtain a contradiction by showing $m' \equiv m \pmod{7^{\ell+1}}$.

For α, β, and γ in R, define $\alpha \equiv \beta \pmod{\gamma}$ to mean that $\gamma | (\alpha - \beta)$ in R. Observe that if a, b, and c are in $\mathbb{Z}$ and $a \equiv b \pmod{c}$ (in $\mathbb{Z}$), then $a \equiv b \pmod{c}$ in R. Also, if a, b, and c are in $\mathbb{Z}$ and $a \equiv b \pmod{c}$ in R, then there is a $\delta \in R$ such that $a - b = c\delta$. In this case, $c = 0$ or $\delta = (a-b)/c \in \mathbb{Q}$. If the latter holds, Theorem 2 implies that $\delta \in \mathbb{Z}$ since δ is an algebraic integer. It follows that $a \equiv b \pmod{c}$ (in $\mathbb{Z}$). Thus, our notion of congruences in R is equivalent to the notion of congruences in $\mathbb{Z}$ in the case that the elements of R are from $\mathbb{Z}$. Since $m' \equiv m \pmod{21}$, $3 | (m' - m)$. Also, $7^\ell | (m' - m)$, so $(3 \times 7^\ell) | (m' - m)$. Note that $\phi(7^{\ell+1}) = 7^{\ell+1} - 7^\ell = 6 \times 7^\ell$. It follows that

$$(2^{3\times 7^\ell} + 1)(2^{3\times 7^\ell} - 1) \equiv 2^{6\times 7^\ell} - 1 \equiv 0 \pmod{7^{\ell+1}}.$$

Since $2^{3\times 7^\ell} + 1 \equiv 1 + 1 \equiv 2 \pmod{7}$, we obtain 7 does not divide $2^{3\times 7^\ell} + 1$. We deduce that $2^{3\times 7^\ell} \equiv 1 \pmod{7^{\ell+1}}$. Since $(3 \times 7^\ell) | (m' - m)$, $2^{m'-m} \equiv 1 \pmod{7^{\ell+1}}$.

If k is an integer > 4, the largest power of 7 dividing $k!$ is 7^r where

$$r = \left[\frac{k}{7}\right] + \left[\frac{k}{7^2}\right] + \cdots < k\Big(\frac{1}{7} + \frac{1}{7^2} + \cdots\Big) = \frac{k}{6} < \frac{k-3}{2}.$$

Since $(\sqrt{-7})^k = \pm 7^{(k-3)/2} \times 7\sqrt{-7}$, we deduce that

$$\begin{aligned}(1+\sqrt{-7})^{m'-m} &\equiv 1 + \sqrt{-7}(m'-m) - 7\binom{m'-m}{2} - 7\sqrt{-7}\binom{m'-m}{3} + \cdots \\ &\equiv 1 + (m'-m)\sqrt{-7} \pmod{7^{\ell+1}}.\end{aligned}$$

Similarly,

$$(1-\sqrt{-7})^{m'-m} \equiv 1 - (m'-m)\sqrt{-7} \pmod{7^{\ell+1}}.$$

With α and β as before,

$$\begin{aligned}\alpha^{m'} \equiv 2^{m'-m}\alpha^{m'} &\equiv \alpha^m (2\alpha)^{m'-m} \equiv \alpha^m (1+\sqrt{-7})^{m'-m} \\ &\equiv \alpha^m (1 + (m'-m)\sqrt{-7}) \pmod{7^{\ell+1}}\end{aligned}$$

and, similarly,

$$\beta^{m'} \equiv \beta^m (1 - (m'-m)\sqrt{-7}) \pmod{7^{\ell+1}}.$$

Hence,

$$\alpha^{m'} - \beta^{m'} \equiv \alpha^m - \beta^m + (\alpha^m + \beta^m)(m'-m)\sqrt{-7} \pmod{7^{\ell+1}}.$$

Since $(**)$ holds as is and with m' replacing m, we obtain

$$\alpha^{m'} - \beta^{m'} = -\sqrt{-7} = \alpha^m - \beta^m.$$

Hence,

$$(\alpha^m + \beta^m)(m'-m)\sqrt{-7} \equiv 0 \pmod{7^{\ell+1}}.$$

This implies that

$$(\alpha^m + \beta^m)(m' - m) \equiv 0 \pmod{\sqrt{-7}^{2\ell+1}}.$$

Since $\sqrt{-7}$ has norm 7, $\sqrt{-7}$ is prime in R. Assume $\sqrt{-7}|(\alpha^m + \beta^m)$. Since (∗∗) implies $\sqrt{-7}|(\alpha^m - \beta^m)$, we deduce that $\sqrt{-7}|(2\alpha)^m$. Taking norms, we obtain $7|8^m$, a contradiction. Therefore,

$$m' - m \equiv 0 \pmod{\sqrt{-7}^{2\ell+1}}.$$

Taking norms, we deduce now that $7^{2\ell+1}|(m'-m)^2$ (in $\mathbb{Z}$) so that $7^{\ell+1}|(m'-m)$. This contradicts our choice of ℓ, completing the proof. ∎

• Mersenne Primes. Another application we now consider is to "large" primes. More specifically, we consider Mersenne numbers $M_n = 2^n - 1$. Typically, in recent years, the largest known prime has been a Mersenne number (an unusual exception was found in 1989). Currently (as of 03/05/00), the largest known prime is M_p where $p = 6972593$ (it has over two million digits). It is easy to see that if M_n is prime, then n must be prime. The reason Mersenne numbers are easy to test for primality is because of the following test (where p denotes an odd prime):

Let $a_1 = 4$ and $a_{m+1} = a_m^2 - 2$ for all integers $m \geq 1$. Then M_p is a prime if and only if $a_{p-1} \equiv 0 \pmod{M_p}$.

Example: Consider $M_{19} = 524287$. Doing arithmetic modulo M_{19}, we obtain

$$\begin{gathered}
a_1 = 4, a_2 = 14, a_3 = 194, a_4 = 37634, a_5 = 218767, \\
a_6 = 47859000287 \equiv 510066 \pmod{M_{19}}, \\
a_7 = 510066^2 - 2 = 260167324354 \equiv 386344 \pmod{M_{19}}, \\
a_8 \equiv 323156 \pmod{M_{19}}, \qquad a_9 \equiv 218526 \pmod{M_{19}}, \\
a_{10} \equiv 504140 \pmod{M_{19}}, \qquad a_{11} \equiv 103469 \pmod{M_{19}}, \\
a_{12} \equiv 417706 \pmod{M_{19}}, \qquad a_{13} \equiv 307417 \pmod{M_{19}}, \\
a_{14} \equiv 382989 \pmod{M_{19}}, \qquad a_{15} \equiv 275842 \pmod{M_{19}}, \\
a_{16} \equiv 85226 \pmod{M_{19}}, \qquad a_{17} \equiv 523263 \pmod{M_{19}}, \\
\text{and} \quad a_{18} \equiv 0 \pmod{M_{19}}.
\end{gathered}$$

Hence, M_{19} is prime.

To check if M_p is prime as above takes $p-1$ steps. Although the numbers a_m may get very large, one can compute the a_m modulo M_p. Roughly, speaking, $a_m \approx 2^{2^m}$ so that computing modulo M_p helps considerably. We will not prove the above but rather a slightly easier result given next. We note that in the result above as well as the next the condition that p is a prime is not necessary (but presumably what is of interest).

Theorem 65. *Let p be a prime $\equiv 3 \pmod 4$. Define $a_1 = 3$ and $a_{m+1} = a_m^2 - 2$ for all integers $m \geq 1$. Then M_p is a prime if and only if $a_{p-1} \equiv 0 \pmod{M_p}$.*

For the proof, we set $\omega = (1+\sqrt{5})/2$ so that the ring of algebraic integers in $\mathbb{Q}(\sqrt{5})$ is $R = \mathbb{Z}[\omega]$. By Theorem 57, R is Euclidean. By Theorem 55, R is a UFD. By Theorem 52 (and a homework problem), irreducibles and primes are the same in R. Setting $\overline{\omega} = (1-\sqrt{5})/2$, we observe that

$$\omega^2 + \overline{\omega}^2 = 3 = a_1$$

and

$$\omega^{2^{m+1}} + \overline{\omega}^{2^{m+1}} = \left(\omega^{2^m} + \overline{\omega}^{2^m}\right)^2 - 2(\omega\overline{\omega})^{2^m} = \left(\omega^{2^m} + \overline{\omega}^{2^m}\right)^2 - 2.$$

It follows by induction that

$$a_m = \omega^{2^m} + \overline{\omega}^{2^m} \qquad \text{for all positive integers } m.$$

We use $N(x)$ to denote the norm function $N_{\mathbb{Q}(\sqrt{5})}(x)$.

Lemma 1. *Let q be a rational prime with $q \neq 2$ and $q \equiv \pm 2 \pmod 5$. Then q is a prime in R and there are no solutions (i.e., $x \in \mathbb{Z}$) to the congruence $x^2 \equiv 5 \pmod q$.*

Proof. Assume q is not prime in R. Then there are β and γ in R such that $q = \beta\gamma$, $|N(\beta)| > 1$, and $|N(\gamma)| > 1$. This implies $|N(\beta)| = |N(\gamma)| = q$. Writing $\beta = (a + b\sqrt{5})/2$, we deduce that $a^2 - 5b^2 = \pm 4q$ so that $a^2 \equiv \pm 4q \pmod 5$. Since $q \equiv \pm 2 \pmod 5$, we obtain a contradiction as ± 3 are not squares modulo 5. Hence, q is a prime in R.

Now, assume $a^2 \equiv 5 \pmod q$ for some integer a. Then q prime in R and $q|(a+\sqrt{5})(a-\sqrt{5})$ implies $q|(a+\sqrt{5})$ or $q|(a-\sqrt{5})$. This gives a contradiction as neither $(a+\sqrt{5})/q$ nor $(a-\sqrt{5})/q$ are in R (as $q > 2$). Thus, there are no solutions to the congruence $x^2 \equiv 5 \pmod q$. ■

Lemma 2. *Let q be a rational prime with $q \neq 2$ and $q \equiv \pm 2 \pmod 5$. Then*

$$5^{(q-1)/2} \equiv -1 \pmod q.$$

Proof. From Lemma 1, there are no solutions to the congruence $x^2 \equiv 5 \pmod q$. Hence, the numbers $\{1, 2, \dots, q-1\}$ can be paired so that each pair (x, y) satisfies $xy \equiv 5 \pmod q$. There are $(q-1)/2$ such pairs, and we deduce

$$5^{(q-1)/2} \equiv (q-1)! \equiv -1 \pmod q$$

by Wilson's Theorem. ■

Lemma 3. *Let q be a rational prime with $q \neq 2$ and $q \equiv \pm 2 \pmod 5$. If $\beta \in R$, then*

$$\beta^{q+1} \equiv N(\beta) \pmod q.$$

Proof. Write $2\beta = a + b\sqrt{5}$ where a and b are in $\mathbb{Z}$. From Fermat's Little Theorem and Lemma 2, we deduce that

$$\begin{aligned} 2\beta^q &\equiv (2\beta)^q \equiv \big(a + b\sqrt{5}\big)^q \\ &\equiv a^q + 5^{(q-1)/2} b^q \sqrt{5} \equiv a - b\sqrt{5} \equiv 2\left(\frac{a - b\sqrt{5}}{2}\right) \pmod{q}. \end{aligned}$$

By Lemma 1, $q \neq 2$ is a prime in R so that

$$\beta^q \equiv \frac{a - b\sqrt{5}}{2} \pmod{q}.$$

Hence,

$$\beta^{q+1} = \beta\beta^q \equiv \left(\frac{a + b\sqrt{5}}{2}\right)\left(\frac{a - b\sqrt{5}}{2}\right) \equiv N(\beta) \pmod{q},$$

completing the proof. ■

Proof of Theorem 65. Since $p \equiv 3 \pmod 4$, we obtain

$$M_p \equiv 2^p - 1 \equiv 2^3\big(2^{p-3}\big) - 1 \equiv 8 - 1 \equiv 2 \pmod 5.$$

Suppose that M_p is prime. Using Lemma 3 with $\beta = \omega$ and $q = M_p$, we obtain

$$\omega^{2^p} \equiv \omega^{M_p+1} \equiv N(\omega) \equiv -1 \pmod{M_p}.$$

Thus,

$$a_{p-1} \equiv \omega^{2^{p-1}} + \overline{\omega}^{2^{p-1}} \equiv \overline{\omega}^{2^{p-1}}\big(\omega^{2^p}(\omega\overline{\omega})^{-2^{p-1}} + 1\big) \equiv \overline{\omega}^{2^{p-1}}\big(\omega^{2^p} + 1\big) \equiv 0 \pmod{M_p}.$$

Now, suppose that we are given that $a_{p-1} \equiv 0 \pmod{M_p}$ and we want to prove that M_p is prime. Then

$$\omega^{2^p} + 1 \equiv \omega^{2^{p-1}}\big(\omega^{2^{p-1}} + \overline{\omega}^{2^{p-1}}\big) \equiv \omega^{2^{p-1}} a_{p-1} \equiv 0 \pmod{M_p}.$$

Hence,

$$\omega^{2^p} \equiv -1 \pmod{M_p} \quad \text{and} \quad \omega^{2^{p+1}} \equiv \big(\omega^{2^p}\big)^2 \equiv 1 \pmod{M_p}.$$

It follows that if $\omega^k \equiv 1 \pmod{M_p}$, then $2^{p+1}|k$. Since $M_p \equiv 2 \pmod 5$, there is a prime divisor $q \equiv \pm 2 \pmod 5$ of M_p. Since M_p is odd, $q \neq 2$. From Lemma 3, we obtain

$$\omega^{2(q+1)} \equiv \big(N(\omega)\big)^2 \equiv 1 \pmod{q}.$$

Therefore, $2^{p+1}|\big(2(q+1)\big)$ so that $2^p|(q+1)$. In other words, $q = 2^p\ell - 1$ for some $\ell \in \mathbb{Z}$. Since $q|M_p$, we deduce that $q \leq 2^p - 1$. Hence, $\ell = 1$ and $q = M_p$. Thus, M_p is prime. ■

Homework:

(1) Let $f_0 = 0$, $f_1 = 1$, and $f_{m+1} = f_m + f_{m-1}$ for every integer $m \geq 1$.

(a) Prove that $f_m = (\omega^m - \overline{\omega}^m)/\sqrt{5}$ for every integer $m \geq 0$.

(b) Using Lemma 3, prove that if q is a rational prime (possibly even) and $q \equiv \pm 2 \pmod 5$, then $q | f_{q+1}$.

Ideal Theory:

• Are ideals ideal? Let $\mathbb{Q}(\alpha)$ be an algebraic extension of $\mathbb{Q}$. Let R be its ring of integers. Let $f(x)$ be the minimal polynomial of α, and suppose $\deg f = n$. The applications we just considered make clear the number theoretic importance of R being a UFD. In fact, a fairly easy argument can be given to prove Fermat's Last Theorem if one assumes (incorrectly) that there exists unique factorization in $\mathbb{Z}[\zeta_p]$ where $\zeta_p = e^{2\pi i/p}$ and p is a prime (recall Theorem 47). But unique factorization does not always exist in R. The importance of considering ideals in R rather than the elements of R is simple; it turns out that there is unique factorization among the ideals in R. Sometimes one can make use of this important feature of ideals in R and obtain rather general number theoretic theorems. Thus, in some sense ideals are indeed ideal. We will establish that unique factorization exists for the ideals in R momentarily, but first we establish some preliminary results.

• What do ideals look like in R? An answer to this question is given by our next theorem. We make use of the notion mentioned above.

Theorem 66. *If $I \neq (0)$ is an ideal in R, then there exists $\beta_1, \beta_2, \dots, \beta_n \in I$ such that every element of I can be uniquely represented in the form*

$$(*) \qquad k_1\beta_1 + k_2\beta_2 + \cdots + k_n\beta_n$$

where $k_1, k_2, \dots, k_n \in \mathbb{Z}$.

Proof. Let $\beta \neq 0$ be an element of I. Since $N(\beta)/\beta$ is in $\mathbb{Q}(\alpha)$ and is an algebraic integer, we deduce that $N(\beta)/\beta \in R$. Hence, $|N(\beta)| = \pm\beta(N(\beta)/\beta) \in I$. Thus, there exists a positive integer in I. Let a denote the smallest positive integer in I. Let $\omega_1, \omega_2, \dots, \omega_n$ be an integral basis for R. Then $a\omega_j \in I$ for each $j \in \{1, 2, \dots, n\}$. Let a_{11} be the smallest positive integer such that $a_{11}\omega_1 \in I$, and let $\beta_1 = a_{11}\omega_1$. Let a_{21} and a_{22} be in $\mathbb{Z}$ with $a_{21} \geq 0$, $a_{22} > 0$, and a_{22} as small as possible with $\beta_2 = a_{21}\omega_1 + a_{22}\omega_2 \in I$ (by considering $a_{21} = 0$ and $a_{22} = a$, we see that such a_{21} and a_{22} exist). Note that by considering $\beta_2 - k\beta_1$ for some $k \in \mathbb{Z}$, we may also suppose that $a_{21} < a_{11}$. In general, for $i \in \{1, 2, \dots, n\}$, define

$$\beta_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \cdots + a_{ii}\omega_i \in I$$

with $0 \leq a_{ij} < a_{jj}$ for $j \in \{1, 2, \dots, i-1\}$ and $a_{ii} > 0$ as small as possible. Observe that $a_{ii} \leq a$ for all $i \in \{1, 2, \dots, n\}$ and, hence, $a_{ij} \leq a$ for all i and j with $1 \leq j \leq i \leq n$. Define $a_{ij} = 0$ for i and j satisfying $1 \leq i < j \leq n$.

Let $\beta \in I$. By the minimality of a_{nn}, there exists $k_n \in \mathbb{Z}$ such that $\beta - k_n\beta_n$ can be written as a linear combination of $\omega_1, \omega_2, \dots, \omega_{n-1}$ over $\mathbb{Z}$. Furthermore, we get $k_{n-1} \in$

$\mathbb{Z}$ such that $\beta - k_{n-1}\beta_{n-1} - k_n\beta_n$ is a linear combination of $\omega_1, \omega_2, \ldots, \omega_{n-2}$ over $\mathbb{Z}$. Continuing, we deduce that there are $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ such that $(*)$ holds.

Now, assume that some $\beta \in I$ has two representations of the form $(*)$. Taking the difference of these two representations, we obtain that there are $k'_1, k'_2, \ldots, k'_n \in \mathbb{Z}$ with some $k'_j \neq 0$ such that

$$k'_1\beta_1 + k'_2\beta_2 + \cdots + k'_n\beta_n = 0.$$

If $\beta_j^{(i)}$ denotes the ith field conjugate of β_j for i and j in $\{1, 2, \ldots, n\}$, then

$$k'_1\beta_1^{(i)} + k'_2\beta_2^{(i)} + \cdots + k'_n\beta_n^{(i)} = 0.$$

Thus, the system of equations

$$x_1\beta_1^{(i)} + x_2\beta_2^{(i)} + \cdots + x_n\beta_n^{(i)} = 0 \qquad \text{for } i \in \{1, 2, \ldots, n\}$$

has a non-trivial solution. It follows that $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = 0$. On the other hand, by the lemma to Theorem 41, we deduce

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = a_{11}^2 a_{22}^2 \cdots a_{nn}^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n) \neq 0.$$

This contradiction implies the uniqueness condition in the theorem holds. ■

Comment: Given the condition $\beta_1, \beta_2, \ldots, \beta_n \in I$, clearly every number of the form given in $(*)$ for $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ is in R.

Corollary. *A non-zero rational integer occurs in only finitely many ideals in R.*

Proof. Since a is in an ideal if and only if $-a$ is in the ideal, it suffices to consider a positive rational integer a. We do so. Each ideal $I \neq (0)$ in R that contains a can be written in the form $\beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$ where

$$\beta_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \cdots + a_{ii}\omega_i \qquad \text{for } i \in \{1, 2, \ldots, n\}$$

where $0 \leq a_{ij} \leq a_{jj} \leq a$ for all i and j with $1 \leq j \leq i \leq n$ and where $\omega_1, \omega_2, \ldots, \omega_n$ is some fixed integral basis for R. This clearly means that there exist finitely many (certainly no more than $(a+1)^{n^2}$) choices for $\beta_1, \beta_2, \ldots, \beta_n \in R$ as above such that $I = \beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$ contains the element a. Since every ideal I in R can be written in this form, the Corollary follows. ■

Homework:

(1) Let $\beta \in R$ where R is a ring of algebraic integers in a number field. Generalize the corollary above by showing that if $\beta \neq 0$, then β occurs in only finitely many ideals in R.

• Multiplication of Ideals. Note that if I is an ideal in R and $\beta_1, \beta_2, \ldots, \beta_n$ are as in Theorem 66, then

$$I = \beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z} \subseteq \beta_1 R + \beta_2 R + \cdots + \beta_n R = (\beta_1, \beta_2, \ldots, \beta_n) \subseteq I.$$

Thus, every ideal in R can be written as an ideal generated by n (or fewer) elements. Let $B = (\beta_1, \beta_2, \ldots, \beta_r)$ and $C = (\gamma_1, \gamma_2, \ldots, \gamma_s)$ be two ideals in R. We define BC as the ideal generated by $\beta_i\gamma_j$ where $1 \leq i \leq r$ and $1 \leq j \leq s$. Before proceeding, we justify that this definition is well-defined, that is that the definition is independent of the generators chosen for B and C. Let D denote the ideal generated by the numbers $\beta_i\gamma_j$ with $1 \leq i \leq r$ and $1 \leq j \leq s$. Suppose $B = (\beta'_1, \beta'_2, \ldots, \beta'_{r'})$ and $C = (\gamma'_1, \gamma'_2, \ldots, \gamma'_{s'})$, and let D' be the ideal generated by the numbers $\beta'_i\gamma'_j$. Sine $\beta'_i \in B$ and $\gamma'_j \in C$ for each $i \in \{1, 2, \ldots, r'\}$ and $j \in \{1, 2, \ldots, s'\}$, we get that for each such fixed i and j there are $u_1, u_2, \ldots, u_r \in R$ and $v_1, v_2, \ldots, v_s \in R$ such that

$$\beta'_i = u_1\beta_1 + u_2\beta_2 + \cdots + u_r\beta_r \quad \text{and} \quad \gamma'_i = v_1\gamma_1 + v_2\gamma_2 + \cdots + v_s\gamma_s.$$

One deduces that $\beta'_i\gamma'_j \in D$. Thus, $D' \subseteq D$. Similarly, $D \subseteq D'$, and we deduce $D = D'$. Thus, the definition of BC does not depend on the generators chosen for B and C.

Note that $\beta \in B$ and $\gamma \in C$ implies $\beta\gamma \in BC$. Also, $BC = CB$.

Theorem 67. *For any ideal B in R, there exists an ideal $C \neq (0)$ in R such that $BC = (a)$ for some $a \in \mathbb{Z}$.*

To prove Theorem 67, we will make use of a few lemmas.

Lemma 1. *Suppose $g(x)$ is a polynomial with all its coefficients from a number field $\mathbb{Q}(\alpha)$ and that $h(x)$ is a polynomial with complex coefficients such that $g(x)h(x)$ is a polynomial with all its coefficients in $\mathbb{Q}(\alpha)$. Then $h(x)$ has all its coefficients in $\mathbb{Q}(\alpha)$.*

Proof. We may suppose (and do suppose) that $g(0) \neq 0$. Write $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$ so that each b_j is in $\mathbb{Q}(\alpha)$ and each c_j is in $\mathbb{C}$. Assume that $h(x)$ has a coefficient that is not in $\mathbb{Q}(\alpha)$, and let k be the least non-negative integer for which $c_k \notin \mathbb{Q}(\alpha)$. Define $c_j = 0$ if $j < 0$. Then the coefficient of x^k in $g(x)h(x)$ is

$$d = b_0c_k + b_1c_{k-1} + \cdots + b_rc_{k-r}$$

where each term other than the first is in $\mathbb{Q}(\alpha)$. Since $g(x)h(x) \in \mathbb{Q}(\alpha)[x]$, we also know $d \in \mathbb{Q}(\alpha)$. But then since $b_0 \in \mathbb{Q}(\alpha)$ and $b_0 \neq 0$, we deduce

$$c_k = \big(d - (b_1c_{k-1} + \cdots + b_rc_{k-r})\big)/b_0 \in \mathbb{Q}(\alpha),$$

a contradiction. Therefore, $h(x)$ has all its coefficients in $\mathbb{Q}(\alpha)$. ■

Lemma 2. *Let $g(x)$ be a polynomial with algebraic integer coefficients, and let ρ be a root of $g(x)$. Then the coefficients of $g(x)/(x-\rho)$ are all algebraic integers.*

Proof. Write

$$g(x) = \tau_0 + \tau_1x + \cdots + \tau_mx^m.$$

We prove the result by induction on m. If $m = 1$, then $g(x) = \tau_1(x-\rho)$ so that $g(x)/(x-\rho) = \tau_1$, an algebraic integer. Suppose the result holds for $m \leq n$ for some positive integer n, and consider $g(x)$ as above with $m = n+1$. Set $w(x) = g(x) - \tau_mx^{m-1}(x-\rho)$. Having taken the comment after Theorem 6 seriously, we see that $w(x)$ has each coefficient being an algebraic integer (in other words, $\tau_m \rho$ satisfies a monic polynomial with algebraic integer coefficients - the reader should verify that this implies $\tau_m \rho$ is therefore an algebraic integer). Furthermore, $\deg w \le m - 1$ and ρ is a root of $w(x)$. Since

$$\frac{g(x)}{x-\rho} = \frac{w(x)}{x-\rho} + \tau_m x^{m-1},$$

the induction hypothesis can be used to finish the proof. ■

Our next lemma generalizes Theorem 6.

Lemma 3. *Let $g(x)$ be a polynomial with algebraic integer coefficients, and suppose the roots of $g(x)$ are $\rho_1, \rho_2, \dots, \rho_m$ so that*

$$g(x) = \tau_m (x-\rho_1)(x-\rho_2)\cdots(x-\rho_m)$$

(where τ_m is the leading coefficient of $g(x)$). If each of $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$ is in $\{0,1\}$, then

$$(*) \qquad \tau_m \rho_1^{\varepsilon_1} \rho_2^{\varepsilon_2} \cdots \rho_m^{\varepsilon_m}$$

is an algebraic integer.

Proof. We do induction on m. The case $m = 1$ is easily handled as then we are given that the coefficients of $g(x) = \tau_1 x - \tau_1 \rho_1$ are algebraic integers. Now, suppose the result holds for $m \le n$ and consider the case when $m = n+1$. If every $\varepsilon_j = 1$, then $(*)$ is plus or minus the constant term of $g(x)$ and, hence, an algebraic integer. If it is not the case that every $\varepsilon_j = 1$, then fix a subscript k such that $\varepsilon_k = 0$ and set $\rho = \rho_k$. By Lemma 2, the coefficients of $h(x) = g(x)/(x-\rho)$ are all algebraic integers. Since $\deg h \le m - 1 = n$, the induction hypothesis now implies the desired result. ■

Lemma 4. *Let R be the ring of algebraic integers in an algebraic number field, and suppose*

$$g(x) = \beta_0 + \beta_1 x + \cdots + \beta_r x^r \in R[x] \quad \text{and} \quad h(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_s x^s \in R[x]$$

with $\beta_r \gamma_s \ne 0$. If $\delta \in R$ divides each coefficient in the product

$$g(x)h(x) = \delta_0 + \delta_1 x + \cdots + \delta_{r+s} x^{r+s} \in R[x],$$

then δ divides each $\beta_i \gamma_j$ where $i \in \{0,1,\dots,r\}$ and $j \in \{0,1,\dots,s\}$.

Proof. Let $\rho_1, \rho_2, \dots, \rho_r$ be the roots of $g(x)$ and $\rho_1', \rho_2', \dots, \rho_s'$ be the roots of $h(x)$. Then the coefficients of

$$\frac{g(x)h(x)}{\delta} = \frac{\beta_r \gamma_s}{\delta}(x-\rho_1)(x-\rho_2)\cdots(x-\rho_r)(x-\rho_1')(x-\rho_2')\cdots(x-\rho_s')$$

are in R by the definition of δ. By Lemma 3,

$$(**) \qquad \frac{\beta_r \gamma_s}{\delta} \rho_1^{\varepsilon_1} \rho_2^{\varepsilon_2} \cdots \rho_r^{\varepsilon_r} (\rho_1')^{\varepsilon_1'} (\rho_2')^{\varepsilon_2'} \cdots (\rho_s')^{\varepsilon_s'}$$

is an algebraic integer for every choice of $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r, \varepsilon_1', \varepsilon_2', \dots, \varepsilon_s'$ in $\{0,1\}$. Also, for every $i \in \{1,2,\dots,r\}$ and $j \in \{1,2,\dots,s\}$, the number β_i/β_r is an elementary symmetric function in $\rho_1, \rho_2, \dots, \rho_r$ and the number γ_j/γ_s is an elementary symmetric function in $\rho_1', \rho_2', \dots, \rho_s'$. Thus, for such i and j,

$$\frac{\beta_i\gamma_j}{\delta} = \frac{\beta_r\gamma_s}{\delta}\frac{\beta_i}{\beta_r}\frac{\gamma_j}{\gamma_s}$$

is a sum of numbers of the form $(**)$ so that $\beta_i\gamma_j/\delta$ is an algebraic integer. Clearly, $\beta_i\gamma_j/\delta \in \mathbb{Q}(\alpha)$. Hence, $\beta_i\gamma_j/\delta \in R$. Thus, δ divides $\beta_i\gamma_j$ for every $i \in \{1,2,\dots,r\}$ and $j \in \{1,2,\dots,s\}$. ■

Proof of Theorem 67. If $B = (0)$, then take $C = (1)$. Now, suppose $B \neq (0)$. Write $B = (\beta_1, \beta_2, \dots, \beta_r)$ with each $\beta_j \neq 0$. Let $g(x) = \beta_1 + \beta_2 x + \cdots + \beta_r x^{r-1}$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be the conjugates of α. Write each β_j as a polynomial in α of degree $\leq n-1$ with coefficients in $\mathbb{Q}$. Define $\beta_j^{(i)}$ as the ith field conjugate of β_j obtained by replacing the polynomial in α representing β_j by the corresponding polynomial in α_i. Define γ_j by

$$h(x) = \prod_{i=2}^{n}\left(\beta_1^{(i)} + \beta_2^{(i)}x + \cdots + \beta_r^{(i)}x^{r-1}\right) = \gamma_1 + \gamma_2 x + \cdots + \gamma_s x^{s-1}.$$

Note that each coefficient of $g(x)h(x)$ is a symmetric polynomial in $\alpha_1, \alpha_2, \dots, \alpha_n$ and each coefficient is an algebraic integer. Hence, $g(x)h(x) \in \mathbb{Z}[x]$. Lemma 1 implies that $h(x)$ has its coefficients in $\mathbb{Q}(\alpha)$. Since the coefficients are also algebraic integers, we deduce that $h(x) \in R[x]$. From the definition of γ_1, we see that $\gamma_1 \neq 0$. We may also suppose that $\gamma_s \neq 0$. Define $b_0, b_1, \dots, b_{r+s-2}$ by

$$g(x)h(x) = b_0 + b_1 x + \cdots + b_{r+s-2}x^{r+s-2}.$$

Set $C = (\gamma_1, \gamma_2, \dots, \gamma_s) \neq (0)$ and $a = \gcd(b_0, b_1, \dots, b_{r+s-2})$. We prove $BC = (a)$. Clearly, the coefficients $b_0, b_1, \dots, b_{r+s-2}$ of

$$g(x)h(x) = \left(\beta_1 + \beta_2 x + \cdots + \beta_r x^{r-1}\right)\left(\gamma_1 + \gamma_2 x + \cdots + \gamma_s x^{s-1}\right)$$

are in BC so that a, being a linear combination of $b_0, b_1, \dots, b_{r+s-2}$ over $\mathbb{Z}$, is in BC. Thus, $(a) \subseteq BC$. To establish that $BC \subseteq (a)$, it suffices to show that each $\beta_i\gamma_j \in (a)$ where $i \in \{1,2,\dots,r\}$ and $j \in \{1,2,\dots,s\}$. This follows as a consequence of Lemma 4. Hence, $BC = (a)$, as desired. ■

• Division by ideals. In this section, we describe some division properties of ideals. We keep to the notation that R is the ring of algebraic integers in an algebraic number field.

Theorem 68. *Let B, C, and D be ideals in R with $D \neq (0)$. If $BD = CD$, then $B = C$.*

Proof. By Theorem 67, there is an ideal $E \neq (0)$ of R such that $DE = (a)$ for some $a \in \mathbb{Z}$. Note that $a \neq 0$. Since $BDE = CDE$, we deduce $B(a) = C(a)$. It follows that for every $b \in B$, there is a $c \in C$ such that $ba = ca$. Thus, $b = c \in C$. Hence, $B \subseteq C$. Similarly, $C \subseteq B$ so that $B = C$. ■

Theorem 69. *Let B and C be ideals in R. Then $B|C$ if and only if $C \subseteq B$.*

Proof. If $B|C$, then there is an ideal D in R such that $BD = C$. Thus, $C \subseteq BD \subseteq BR \subseteq B$. Now, suppose we know $C \subseteq B$ and that we want to prove $B|C$. Since $C \subseteq B$, we have $CE \subseteq BE$ for every ideal E of R. By Theorem 67, there is such an E with $E \neq (0)$ and $BE = (a)$ where $a \in \mathbb{Z}$. Write $CE = (u_1, u_2, \ldots, u_r)$. Since $CE \subseteq BE = (a)$, for each u_j, there is a $v_j \in R$ such that $u_j = av_j$. Hence,

$$\begin{aligned} CE &= (u_1, u_2, \ldots, u_r) = (a)(v_1, v_2, \ldots, v_r) \\ &= BE(v_1, v_2, \ldots, v_r) = B(v_1, v_2, \ldots, v_r)E. \end{aligned}$$

It follows from Theorem 68 that $C = B(v_1, v_2, \ldots, v_r)$. Hence, $B|C$. ■

Theorem 70. *Let $B \neq (0)$ be an ideal in R. Then there exist only finitely many distinct ideals C in R such that $C|B$.*

Proof. As in the beginning of the proof of Theorem 66, there is a non-zero $a \in \mathbb{Z}$ that lies in B. If $C|B$, then Theorem 69 implies $B \subseteq C$ so that $a \in C$. The result now follows from the Corollary to Theorem 66. ■

• Greatest common divisors, prime ideals, and relatively prime ideals. Let B and C be ideals in R. Then an ideal D in R is called a *greatest common divisor of B and C* if (i) D divides both B and C and (ii) for every ideal E in R dividing both B and C, we have $E|D$.

Theorem 71. *Let B and C be ideals in R. Then there exists a unique greatest common divisor of B and C. Furthermore, letting $GCD(B, C)$ denote this greatest common divisor, we have*

$$GCD(B, C) = B + C = \{\beta + \gamma : \beta \in B, \gamma \in C\}.$$

Proof. Let $D = B + C$. We show that D is an ideal, that D is a divisor of B and C, that D is in fact a greatest common divisor of B and C, and finally that there are no other greatest common divisors of B and C. That D is an ideal easily follows from the definition of $B + C$ and the definition of an ideal. Since $0 \in B$ and $0 \in C$, we have $C \subseteq B + C$ and $B \subseteq B + C$ so that $D = B + C$ divides both C and B by Theorem 69. Let E be an ideal in R that divides both B and C. Theorem 69 implies that $B \subseteq E$ and $C \subseteq E$ so that $B + C \subseteq E$. Theorem 69 now implies $E|D$. Thus, D is a greatest common divisor of B and C. If D' is also, then $D|D'$ and $D'|D$. By Theorem 69, we deduce that $D' \subseteq D$ and $D \subseteq D'$. Hence, $D' = D$. It follows that D is *the* greatest common divisor of B and C. ■

Let B and C be ideals in R. If $GCD(B, C) = (1)$, then B and C are said to be relatively prime. If $B \neq (1)$ and the only ideals dividing B are (1) and B, then we say that B is *prime* or a *prime ideal*. Observe that if B is prime, then $B \neq (0)$.

Theorem 72. *If B and C are relatively prime ideals in R, then there exists $\beta \in B$ and $\gamma \in C$ such that $\beta + \gamma = 1$.*

Proof. The result is clear. ■

Theorem 73. *Let B, C, and D be ideals in R with B and C relatively prime. If $B|CD$, then $B|D$.*

Proof. Suppose $B|CD$. By Theorem 69, it suffices to show that $D \subseteq B$. Let $\delta \in D$. By Theorem 72, there are $\beta \in B$ and $\gamma \in C$ such that $\beta + \gamma = 1$. Hence, $\delta = \beta\delta + \gamma\delta$. Note that $\beta \in B$ and $\delta \in R$ implies $\beta\delta \in B$. Also, $B|CD$ implies $CD \subseteq B$ so that $\gamma\delta \in B$. Hence, $\delta = \beta\delta + \gamma\delta \in B$. We deduce $D \subseteq B$. ■

Theorem 74. *Let B be a prime ideal in R. If $B = CD$ where C and D are ideals in R, then either $C = (1)$ or $D = (1)$. If E and F are ideals in R such that $B|EF$, then either $B|E$ or $B|F$.*

Proof. Suppose $B = CD$. Then $C|B$ and, by the definition of a prime ideal, either $C = (1)$ or $C = B$. If $C = B$, then $B(1) = BD$. Since B is prime, $B \neq (0)$. It follows from Theorem 68 then that $D = (1)$. Hence, if $B = CD$, then either $C = (1)$ or $D = (1)$.

Suppose $B|EF$. Let $D' = GCD(B, E)$. Then $D'|B$ so that $D' = (1)$ or $D' = B$. If $D' = (1)$, we deduce from $B|EF$ and Theorem 73 that $B|F$. If $D' = B$, then by the definition of D' we have $B|E$. Hence, if $B|EF$, then either $B|E$ or $B|F$. ■

Homework:

(1) Let n be a positive rational integer. Define a *greatest common divisor for n ideals* $A_1, \ldots, A_n$ in R as an ideal D in R that satisfies (i) D divides each of $A_1, \ldots, A_n$ and (ii) if E is an ideal dividing each of $A_1, \ldots, A_n$, then $E|D$. Prove that such a greatest common divisor is unique. Denote it by $GCD(A_1, \ldots, A_n)$, and furthermore prove that

$$GCD(A_1, \ldots, A_n) = A_1 + A_2 + \cdots + A_n.$$

(2) Prove that if P is a prime ideal in R, then P does not divide (1).

• Unique factorization of ideals. We are now ready to show that even though the ring R of algebraic integers in an algebraic number field $\mathbb{Q}(\alpha)$ is not always a UFD, if we consider the ideals in R, we do always have unique factorization.

Theorem 75. *Every non-zero ideal in R can be written as a finite product of prime ideals. Furthermore, the representation as such a product is unique except possibly for the order in which the factors occur.*

Proof. First, we deal with uniqueness of factorizations into prime ideals. Suppose that

$$P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s$$

for some prime ideals $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_s$. Since $P_1 | Q_1 Q_2 \cdots Q_s$, we deduce from Theorem 74 that $P_1 | Q_j$ for some $j \in \{1, 2, \ldots, s\}$. Since P_1 is prime, $P_1 \neq (1)$. Since Q_j is prime and $P_1 | Q_j$, we obtain $P_1 = Q_j$. We now appeal to Theorem 68 to deduce that

$$P_2 \cdots P_r = Q_1 \cdots Q_{j-1} Q_{j+1} \cdots Q_s.$$

Continuing in this manner, we obtain that $r = s$ (make use of Homework (2) above) and $P_1, \dots, P_r$ is some reordering of $Q_1, \dots, Q_r$.

Let B be an ideal in R. By Theorems 69 and 70, there are only finitely many ideals containing B. If $B = (1)$, then we view B as an empty product of prime ideals. Otherwise, among the finitely many ideals containing B, there is a maximal ideal P_1 so that $B \subseteq P_1 \neq (1)$ and there does not exist another ideal in R other than (1) and P_1 that P_1 is contained in. By Theorem 69, the ideals (1) and P_1 are the only ideals dividing P_1. Hence, P_1 is prime. Since $B \subseteq P_1$, we deduce from Theorem 69 that $P_1 | B$ so that $B = P_1 B_2$ for some ideal B_2 in R. Thus, we can write any ideal $B \neq (1)$ in R as a product of a prime ideal and some ideal. Hence, either $B_2 = (1)$ or there is a prime ideal P_2 in R such that $B = P_1 P_2 B_3$ for some ideal B_3 of R. Continuing in this fashion, we obtain either a factorization of B into a finite product of prime ideals or we obtain, for each positive integer k, prime ideals $P_1, \dots, P_k$ and an ideal B_{k+1} such that $B = P_1 P_2 \cdots P_k B_{k+1}$. We justify the latter cannot happen. Indeed, if $B = P_1 P_2 \cdots P_k B_{k+1}$, then by the uniqueness of factorizations already established we deduce that $P_1, P_1 P_2, \dots, P_1 P_2 \cdots P_k$ are k distinct ideals dividing B. Since k can be arbitrarily large, this contradicts Theorem 70. Thus, B can be expressed as a finite product of prime ideals in R, and such a factorization is unique except for the order in which the factors occur. ■

• An algebraist's nightmare. The next theorem is not true for all rings R; but nevertheless for the ring R of algebraic integers in a number field, the result does hold. We establish the result, but forewarn the reader about mentioning the result as stated below to an algebraist.

Theorem 76. *We have that R is a PID if and only if R is a UFD.*

Lemma. *If π is a prime in R, then (π) is a prime ideal in R.*

Proof. Assume that (π) is not a prime ideal. Then there is an ideal A in R dividing (π) with $A \neq (1)$ and $A \neq (\pi)$. Let B be an ideal with $(\pi) = AB$. Observe that $B \neq (\pi)$; otherwise, $(1)(\pi) = A(\pi)$ implies from Theorem 68 that $A = (1)$, a contradiction. Since $A \neq (\pi)$, there is a $u \in A$ such that $\pi \nmid u$ in R. Since $B \neq (\pi)$, there is a $v \in B$ such that $\pi \nmid v$ in R. On the other hand, $uv \in AB = (\pi)$ so that $\pi | uv$. This contradicts that π is prime. ■

Proof of Theorem 76. By Theorem 54, it suffices to show that if R is a UFD, then R is a PID. Suppose then that R is a UFD. By Theorem 52, primes and irreducibles are the same in R. From Theorem 75, to establish that R is a PID, it suffices to show that every prime ideal in R is principal. Let P be a prime ideal in R. Then $P \neq (0)$ so that there is some $\beta \neq 0$ with $\beta \in P$. By Theorem 50, there exist primes $\pi_1, \pi_2, \dots, \pi_r$ in R such that $\beta = \pi_1 \pi_2 \cdots \pi_r$. Hence,

$$(\beta) = (\pi_1)(\pi_2) \cdots (\pi_r).$$

Also, $(\beta) \subseteq P$ implies $P | (\beta)$. Hence, by Theorem 74, there is a $j \in \{1, 2, \dots, r\}$ such that $P | (\pi_j)$. By the lemma, (π_j) is a prime ideal. Since $P \neq (1)$, we deduce that $P = (\pi_j)$. Therefore, P is principal. ■

• Modulo arithmetic with ideals; norms of ideals. Let A be an ideal in R, the ring of algebraic integers in an algebraic number field. If β and γ are in R, then we say that β *is congruent to* γ *modulo the ideal* A and write $\beta \equiv \gamma \pmod{A}$ if $\beta - \gamma \in A$. Note that $\beta \equiv \gamma \pmod{A}$ if and only if $\beta - \gamma \in A$ if and only if $(\beta - \gamma) \subseteq A$ if and only if $A|(\beta - \gamma)$. For $\beta \in A$, we define the set of $\gamma \in A$ satisfying $\beta \equiv \gamma \pmod{A}$ as the residue class modulo A containing β.

Theorem 77. *There are only finitely many distinct residue classes modulo a given non-zero ideal A in R.*

Proof. By Theorem 67, there is a non-zero ideal B in R such that $AB = (a)$ for some positive $a \in \mathbb{Z}$. By Theorem 69, $A|(a)$ implies $(a) \subseteq A$. Hence, if $\beta_1 \equiv \beta_2 \pmod{(a)}$, then $\beta_1 \equiv \beta_2 \pmod{A}$. In other words, if $\beta_1 \not\equiv \beta_2 \pmod{A}$, then $\beta_1 \not\equiv \beta_2 \pmod{(a)}$. Thus, it suffices to show that (a) has only finitely many residue classes. Let $\omega_1, \dots, \omega_n$ be an integral basis for R. Let $\beta \in R$. Then there exist unique rational integers $b_1, b_2, \dots, b_n$ such that

$$\beta = b_1\omega_1 + b_2\omega_2 + \cdots + b_n\omega_n.$$

If $b'_j \in \{0, 1, \dots, a-1\}$ such that $b_j \equiv b'_j \pmod{a}$ (i.e., over $\mathbb{Z}$), then

$$\beta \equiv b'_1\omega_1 + b'_2\omega_2 + \cdots + b'_n\omega_n \pmod{(a)}.$$

Thus, there are at most a^n distinct residue classes modulo (a), completing the proof. ■

The number of distinct residue classes modulo A is called the *norm of the ideal* A and written $N(A)$ or $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(A)$.

Theorem 78. *If a is a rational positive integer and n is the degree of the minimal polynomial for α, then*

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\big((a)\big) = a^n.$$

Proof. In the proof of Theorem 77, we saw that $N((a)) \le a^n$. More specifically, we showed that every β in R is congruent modulo (a) to some number of the form

$$(*) \qquad b'_1\omega_1 + b'_2\omega_2 + \cdots + b'_n\omega_n \qquad \text{with each } b_j \in \{0, 1, \dots, a-1\},$$

where $\omega_1, \dots, \omega_n$ is an integral basis for R. Suppose β and γ are two numbers of the form given in $(*)$ and that $\beta \equiv \gamma \pmod{(a)}$. Then $\beta - \gamma \in (a)$ so that $\beta - \gamma = ar$ for some $r \in R$. Since $r \in R$, there are rational integers $c_1, c_2, \dots, c_n$ such that $r = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n$ so that

$$\beta - \gamma = ac_1\omega_1 + ac_2\omega_2 + \cdots + ac_n\omega_n.$$

The representation of $\beta - \gamma$ as a linear combination of $\omega_1, \dots, \omega_n$ with rational integer coefficients is unique, and it follows that we must have $\beta = \gamma$. Thus, the numbers of the form in $(*)$ are distinct, and we deduce that $N((a)) \ge a^n$. Therefore, $N((a)) = a^n$. ■

With a little more effort, it is possible to show more generally that if β is an element of R, then

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\big((\beta)\big) = |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)|.$$

We will use Theorem 78 to obtain information about the norm of a prime ideal; the generalization, though certainly of interest, will not be needed in this context.

Theorem 79. *Let $P_1, P_2, \ldots, P_r$ be prime ideals in R. Let*

$$B_i = P_1^{e_{i1}} P_2^{e_{i2}} \cdots P_r^{e_{ir}} \qquad \text{for } i \in \{1, 2, \ldots, m\},$$

where m is a rational integer and each e_{ij} is a non-negative rational integer. Then

$$GCD(B_1, B_2, \ldots, B_m) = \prod_{j=1}^{r} P_j^{\min_{1\le i\le m}\{e_{ij}\}}.$$

Proof. Let $D = GCD(B_1, B_2, \ldots, B_r)$. Let P be a prime ideal in R and f a rational positive integer such that $P^f|D$ and $P^{f+1} \nmid D$. By definition, $D|B_i$ so that $P^f|B_i$ for every $i \in \{1, 2, \ldots, m\}$. We deduce that $P = P_j$ for some $j \in \{1, 2, \ldots, r\}$. Also, $f \le \min_{1\le i\le m}\{e_{ij}\}$. Fix $j \in \{1, 2, \ldots, r\}$, and set $e = \min_{1\le i\le m}\{e_{ij}\}$. Then $P_j^e|B_i$ for every $i \in \{1, 2, \ldots, m\}$. Hence, $P_j^e|D$. The lemma follows. ■

Theorem 80. *If A and B are non-zero ideals in R, then there is a $\beta \in A$ such that $GCD\big((\beta), AB\big) = A$.*

Proof. Let $P_1, \ldots, P_r$ be the prime ideals dividing AB. Write

$$A = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

where e_j are non-negative rational integers. Let

$$B_i = \prod_{\substack{1\le j\le r \\ j\ne i}} P_j^{e_j+1} \qquad \text{for } i \in \{1, 2, \ldots, r\}.$$

By Theorem 79,

$$GCD(B_1, B_2, \ldots, B_r) = (1).$$

Thus, there exist $\beta_i \in B_i$ for $i \in \{1, 2, \ldots, r\}$ such that $\beta_1 + \beta_2 + \cdots + \beta_r = 1$. For $i \in \{1, 2, \ldots, r\}$, $\beta_i \in B_i$ so that $(\beta_i) \subseteq B_i$, $B_i|(\beta_i)$, and, for each $j \in \{1, 2, \ldots, r\}$ with $j \ne i$, we have $P_j^{e_j+1}|(\beta_i)$. Since $(\beta_1) + (\beta_2) + \cdots + (\beta_r) = (1)$, we deduce that $GCD\big((\beta_1), (\beta_2), \cdots (\beta_r)\big) = (1)$. Theorem 79 implies that $P_i \nmid B_i$. Let $\gamma_i \in P_i^{e_i}$ with $\gamma_i \notin P_i^{e_i+1}$. Observe that $P_i^{e_i}|(\beta_i)(\gamma_i)$ and $P_i^{e_i+1} \nmid (\beta_i)(\gamma_i)$. Define

$$\gamma = \beta_1\gamma_1 + \beta_2\gamma_2 + \cdots + \beta_r\gamma_r.$$

Then

$$\begin{aligned}
(\gamma) &\subseteq (\beta_1\gamma_1) + (\beta_2\gamma_2) + \cdots + (\beta_r\gamma_r) \\
&= GCD((\beta_1)(\gamma_1), (\beta_2)(\gamma_2), \ldots, (\beta_r)(\gamma_r)) \\
&= P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r} C = AC \subseteq A,
\end{aligned}$$

where C is an ideal in R with $GCD(C, P_1P_2\cdots P_r) = (1)$. Thus, $A|(\gamma)$.

Let C' be an ideal in R with $(\gamma) = AC'$. We prove $GCD(C', P_1P_2\cdots P_r) = (1)$. In other words, we show that $P_j \nmid C'$ for each $j \in \{1, 2, \ldots, r\}$. Assume some $P_j|C'$. Then $P_j^{e_j+1}|(\gamma)$. We use that $P_j^{e_j+1}|(\beta_i)$ for $i \neq j$ and Theorem 79 to obtain

$$\begin{aligned}
(\beta_j\gamma_j) &= \Bigg(\gamma - \sum_{\substack{1\le i\le r\\ i\neq j}} \beta_i\gamma_i\Bigg)\\
&\subseteq (\gamma) + (\beta_1\gamma_1) + (\beta_2\gamma_2) + \cdots + (\beta_{j-1}\gamma_{j-1}) + (\beta_{j+1}\gamma_{j+1}) + \cdots + (\beta_r\gamma_r)\\
&= GCD\big((\gamma), (\beta_1)(\gamma_1), (\beta_2)(\gamma_2), \ldots, (\beta_{j-1})(\gamma_{j-1}), (\beta_{j+1})(\gamma_{j+1}), \ldots, (\beta_r)(\gamma_r)\big) \subseteq P_j^{e_j+1}.
\end{aligned}$$

Thus, $P_j^{e_j+1}|(\beta_j)(\gamma_j)$, a contradiction.

Since $GCD(C', P_1P_2\cdots P_r) = (1)$, we deduce that $GCD(C', B) = (1)$. Hence,

$$GCD\big((\gamma), AB\big) = GCD\big(AC', AB\big) = A.$$

This completes the proof. ■

Theorem 81. *Let β and γ be in R, and let A be a non-zero ideal of R. Set $D = GCD((\beta), A)$. Then*

$$(*) \qquad \beta x \equiv \gamma \pmod{A}$$

has a solution in R if and only if $D|(\gamma)$. Furthermore, if $D|(\gamma)$, then the solution to $(*)$ is unique modulo A/D.

Proof. Let $\xi \in R$ be a solution to $(*)$. Then $\beta\xi - \gamma \in A$. Since $D|A$, we have $A \subseteq D$ which implies $\beta\xi - \gamma \in D$. Also, $D|(\beta)$ implies $\beta \in (\beta) \subseteq D$ so that $\beta\xi \in D$. It follows that $\gamma \in D$ so that $(\gamma) \subseteq D$ and $D|(\gamma)$.

Now, suppose we know $D|(\gamma)$ and we want to prove $(*)$ has a solution. Then

$$\gamma \in (\gamma) \subseteq D = (\beta) + A$$

so that $\gamma = \beta\omega + \tau$ for some $\omega \in R$ and $\tau \in A$. It follows that $\gamma - \beta\omega \in A$ so that $(*)$ has a solution.

To establish the last part of the theorem, consider ideals B_1 and B_2 in R such that $(\beta) = DB_1$ and $A = DB_2$. Observe that Theorem 79 implies that $GCD(B_1, B_2) = (1)$. Now, suppose ξ_1 and ξ_2 are in R such that

$$\beta\xi_1 \equiv \beta\xi_2 \equiv \gamma \pmod{A}.$$

Then $\beta(\xi_1 - \xi_2) \in A$ so that

$$(\beta)(\xi_1 - \xi_2) = (\beta\xi_1 - \beta\xi_2) \subseteq A.$$

Hence, $DB_2|DB_1(\xi_1 - \xi_2)$. Since $D \neq (0)$, we deduce from Theorem 68 that $B_2|B_1(\xi_1 - \xi_2)$. By Theorem 73, $B_2|(\xi_1 - \xi_2)$ so that $\xi_1 - \xi_2 \in (\xi_1 - \xi_2) \subseteq B_2$. We deduce $\xi_1 \equiv \xi_2 \pmod{B_2}$, which is equivalent to what was to be shown. ■

Theorem 82. *Let A and B be non-zero ideals in R. Then $N(AB) = N(A)N(B)$.*

Proof. By Theorem 80, there is a $\delta \in A$ such that $GCD((\delta), AB) = A$. Let $\beta_1, \dots, \beta_k$ and $\gamma_1, \dots, \gamma_\ell$ be representatives of the complete residue systems modulo A and modulo B respectively so that $N(A) = k$ and $N(B) = \ell$. We prove that $\beta_i + \delta\gamma_j$ for $i \in \{1, 2, \dots, k\}$ and $j \in \{1, 2, \dots, \ell\}$ are representatives for distinct residue classes modulo AB and that every element of R is congruent to some $\beta_i + \delta\gamma_j$ modulo AB. Hence, it will follow that $N(AB) = k\ell = N(A)N(B)$.

If $\beta_i + \delta\gamma_j \equiv \beta_r + \delta\gamma_s \pmod{AB}$, then $\beta_i - \beta_r \equiv \delta(\gamma_s - \gamma_j) \pmod{AB}$. By Theorem 81, $D|(\beta_i - \beta_r)$ where $D = GCD((\delta), AB)$. By the definition of δ, $D = A$. Thus, $\beta_i - \beta_r \in (\beta_i - \beta_r) \subseteq A$ so that $\beta_i \equiv \beta_r \pmod{A}$. It follows that $i = r$. Also, since $0 \equiv \delta(\gamma_s - \gamma_j) \pmod{AB}$, we deduce from Theorem 81 that $\gamma_s - \gamma_j \equiv 0 \pmod{AB/D}$ so that $\gamma_s \equiv \gamma_j \pmod{B}$ and we obtain $s = j$.

Let $\omega \in R$. Then there is an $i \in \{1, 2, \dots, k\}$ such that $\omega \equiv \beta_i \pmod{A}$. Observe that $\omega - \beta_i \in A$ implies $(\omega - \beta_i) \subseteq A$ so that $A|(\omega - \beta_i)$. Since $GCD((\delta), AB) = A$, we obtain from Theorem 81 that there is a $v \in R$ such that $\delta v \equiv \omega - \beta_i \pmod{AB}$. Let $j \in \{1, 2, \dots, \ell\}$ be such that $v \equiv \gamma_j \pmod{B}$. Since $\delta \in A$ and $v - \gamma_j \in B$, we obtain

$$\omega - (\beta_i + \delta\gamma_j) = (\omega - \beta_i) - \delta v + \delta(v - \gamma_j) \in AB$$

so that $\omega \equiv \beta_i + \delta\gamma_j \pmod{AB}$. Thus, every element of R is congruent to some $\beta_i + \delta\gamma_j$ modulo AB, completing the proof. ■

Corollary. *Let A be an ideal in R. If $N(A)$ is prime, then A is a prime ideal.*

This result is an immediate consequence of Theorem 82 upon noting that the only ideal with norm 1 is (1). We had previously seen that $N(\beta)$ prime implies β is irreducible. We can now see that something stronger must hold. The remark after the proof of Theorem 78 implies that if $N(\beta)$ is prime, then so is $N((\beta))$. The Corollary above would then imply that (β) is a prime ideal. If (β) is a prime ideal, then β is a prime in R (why?). Hence, if $N(\beta)$ is prime, then β is a prime in R.

Theorem 83. *Let A be a non-zero ideal in R. Then $N(A) \in A$.*

Proof. Let $\beta_1, \beta_2, \dots, \beta_r$ be representatives of the complete residue system modulo A so that $r = N(A)$. Then $\beta_1 + 1, \beta_2 + 1, \dots, \beta_r + 1$ are all incongruent modulo A and so they are congruent modulo A to $\beta_1, \beta_2, \dots, \beta_r$ in some order. Hence,

$$\begin{aligned} \beta_1 + \beta_2 + \cdots + \beta_r &\equiv \beta_1 + 1 + \beta_2 + 1 + \cdots + \beta_r + 1 \\ &\equiv \beta_1 + \beta_2 + \cdots + \beta_r + r \equiv \beta_1 + \beta_2 + \cdots + \beta_r + N(A) \pmod{A}. \end{aligned}$$

Thus, $N(A) \equiv 0 \pmod{A}$ which implies $N(A) \in A$. ■

Homework:

(1) (A Generalization of Fermat's Little Theorem) Let P be a prime ideal in R. Let $\beta \in R$ with $P \nmid (\beta)$. Prove that

$$\beta^{N(P)-1} \equiv 1 \pmod{P}.$$

Theorem 84. *Let R be the ring of algebraic integers in a number field $\mathbb{Q}(\alpha)$. There are infinitely many prime ideals in R. Each such prime ideal P divides exactly one ideal (p) where p is a rational prime. Furthermore, if $P|(p)$, then $N(P) = p^f$ where $1 \leq f \leq n$ where n is the degree of the minimal polynomial for α.*

Proof. Let p and q be distinct rational primes. Since there are integers x and y satisfying $px + qy = 1$, we deduce $GCD((p),(q)) = (1)$. Since (p) must have a prime ideal divisor and since there exist infinitely many rational primes p, there must exist infinitely many prime ideals. Now, let P be a prime ideal in R. Let $a = N(P)$. By Theorem 83, $a \in P$ so that $(a) \subseteq P$ and $P|(a)$. Write $a = p_1 p_2 \cdots p_r$ where the p_j are (not necessarily distinct) rational primes. Then $P|(a)$ implies $P|(p_1)(p_2)\cdots(p_r)$ so that $P|(p)$ for some $p = p_j$. Hence, there exists an ideal A such that $(p) = PA$. By Theorems 78 and 82, we have

$$N(P)N(A) = N(PA) = N\big((p)\big) = p^n.$$

It follows that $N(P) = p^f$ where $1 \leq f \leq n$. This also establishes that the rational prime p for which $P|(p)$ is unique. ■

Theorem 85. *There are only finitely many ideals in R of a given norm.*

Proof. This follows from the Corollary to Theorem 66 and Theorem 83. ■

- An application of ideals. In this section, we establish

Theorem 86. *Let $a_1, \ldots, a_{n-1}$ denote arbitrary rational integers. Then the polynomial*

$$(*) \qquad \frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_2\frac{x^2}{2!} + a_1 x \pm 1$$

is irreducible over the rationals.

Theorem 86 is due to I. Schur. As a lemma to the theorem, Schur gave a proof of the next result which we will state without proof. The lemma was originally established by Sylvester, and it can be viewed as a generalization of the classical Betrand's Postulate (take $m = k + 1$).

Lemma 1. *Let k and m be positive integers with $m > k$. Then one of the numbers $m, m+1, \ldots, m+k-1$ is divisible by a prime $> k$.*

More simply put, the product of k consecutive integers each larger than k is divisible by a prime larger than k. Both Schur and Sylvester established Lemma 1 by use of analytic methods; Erdős later gave an elementary proof of the lemma. Following Schur, we will make use of algebraic number theory in establishing our next lemma. We first fix a polynomial $f(x)$ as in $(*)$ and define $F(x) = n!f(x)$ so that $F(x) \in \mathbb{Z}[x]$. Observe that if $F(x)$ is reducible over the rationals, then $F(x)$ must have an irreducible factor of some positive degree $k \leq n/2$. To prove the theorem by contradiction, we assume that $F(x) = A(x)B(x)$

with $A(x)$ and $B(x)$ in $\mathbb{Z}[x]$, $A(x)$ is irreducible over $\mathbb{Q}$ of degree k, and $1 \le k \le n/2$ (recall Theorem 8). Since $F(x)$ is monic, we may suppose $A(x)$ and $B(x)$ are as well and do so. Let b_j be rational integers such that

$$A(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0.$$

Lemma 2. *Given the above, every prime divisor of b_0 is $\le k$.*

Before proving Lemma 2, we show how Lemma 1 and Lemma 2 imply that Theorem 86 holds. Observe that $k \le n/2$ implies $n-k+1 \ge k+1 > k$. Setting $m = n-k+1$ in Lemma 1, we deduce that there is a rational prime $p > k$ such that $p|(n-k+1)(n-k+2)\cdots(n-1)n$. It follows that

$$\begin{aligned} F(x) &= x^n + na_{n-1}x^{n-1} + n(n-1)a_{n-2}x^{n-2} + \cdots + n!a_1 x \pm n! \\ &\equiv x^n + na_{n-1}x^{n-1} + n(n-1)a_{n-2}x^{n-2} + \\ &\qquad \cdots + n(n-1)\cdots(n-k+2)a_{n-k+1}x^{n-k+1} \pmod{p}. \end{aligned}$$

On the other hand, $F(x) \equiv A(x)B(x) \pmod{p}$. By unique factorization in $\mathbb{Z}_p[x]$, we deduce that since $\deg B(x) = n-k$, x must divide $A(x)$ modulo p. But this implies $p|b_0$, contradicting Lemma 2 (since $p > k$). We are left then with establishing Lemma 2. First, we prove the following.

Lemma 3. *Let R be the ring of algebraic integers in some algebraic number field. Let $\beta \in R$, and suppose that p is a rational prime dividing $N(\beta)$. Then there is a prime ideal P dividing (p) such that $P|(\beta)$.*

Proof. By Theorem 79, it suffices to show that $GCD((\beta),(p)) \ne (1)$. Assume otherwise. Then $(\beta)+(p) = 1$ so that there are λ_1 and λ_2 in R satisfying $\beta\lambda_1 + p\lambda_2 = 1$. It follows that

$$N(\beta)N(\lambda_1) = N(\beta\lambda_1) = N(1 - p\lambda_2).$$

Since $p|N(\beta)$, we obtain $N(1-p\lambda_2) \equiv 0 \pmod{p}$. On the other hand, if $\lambda_2^{(1)}, \lambda_2^{(2)}, \dots, \lambda_2^{(n')}$ are the field conjugates of λ_2, then

$$N(1-p\lambda_2) \equiv \prod_{j=1}^{n'}(1 - p\lambda_2^{(j)}) \equiv 1 \pmod{p}.$$

Hence, we obtain a contradiction, from which the lemma follows. ■

Proof of Lemma 2. Let α be a root of $A(x)$, and let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Note that $A(x)$ being monic and irreducible implies that $A(x)$ is the minimal polynomial for α. Also, $\alpha \in R$. Let p be a rational prime dividing b_0. Since b_0 is $(-1)^k$ times the product of the roots of $A(x)$, we obtain

$$N(\alpha) \equiv \pm b_0 \equiv 0 \pmod{p}.$$

By Lemma 3, there is a prime ideal P in R such that $P|(\alpha)$ and $P|(p)$. Write

$$(\alpha) = P^r M \qquad \text{and} \qquad (p) = P^s N,$$

where M and N are ideals satisfying $GCD(M,P) = GCD(N,P) = (1)$. Then $r \geq 1$ and, by Theorem 84, $1 \leq s \leq k$. Since $A(\alpha) = 0$, we have $F(\alpha) = 0$ so that

$$(**) \qquad \pm n! + n! a_1 \alpha + \frac{n!}{2!} a_2 \alpha^2 + \cdots + \frac{n!}{(n-1)!} a_{n-1} \alpha^{n-1} + \alpha^n = 0.$$

For each non-negative rational integer $v \leq n$, let

$$h_v = \left[\frac{v}{p}\right] + \left[\frac{v}{p^2}\right] + \left[\frac{v}{p^3}\right] + \cdots .$$

Then h_v is such that $p^{h_v}|v!$ but $p^{h_v+1} \nmid v!$. Define $a_n = 1$ and $a_0 = \pm 1$ so that the coefficient of α^v in $(**)$ is $(n!/v!)a_v$. Consider the term $(n!/v!)a_v\alpha^v$ in $(**)$. Observe that $p^{h_n - h_v}|(n!/v!)$. Since $P^r|(\alpha)$ and $P^s|(p)$,

$$P^{h_n s + rv - h_v s} \quad \text{divides the ideal} \quad (n!/v!)(a_v)(\alpha)^v.$$

We claim that for some $v \in \{1, 2, \ldots, n\}$,

$$(* * *) \qquad rv \leq h_v s.$$

Assume $(* * *)$ does not hold for every $v \in \{1, 2, \ldots, n\}$. Then

$$P^{h_n s+1}|(n!/v!)(a_v)(\alpha)^v \quad \text{for every } v \in \{1, 2, \ldots, n\}.$$

Hence, $P^{h_n s+1}$ divides $GCD((n!)(a_1)(\alpha), (n!/2)(a_2)(\alpha)^2, \ldots, (\alpha)^n)$. Thus, by $(**)$ and Theorem 69,

$$n! \in (n! a_1 \alpha) + \left(\frac{n!}{2} a_2 \alpha^2\right) + \cdots + (\alpha^n) \subseteq GCD((n!)(a_1)(\alpha), \ldots, (\alpha)^n) \subseteq P^{h_n s+1}.$$

By Theorem 69, we also deduce since $(n!) \subseteq P^{h_n s+1}$ that $P^{h_n s+1}|(n!)$. By Theorem 84, P does not divide any ideal (q) with q a rational prime other than $q = p$. From Theorem 75, we deduce that $P^{h_n s}|(n!)$ but $P^{h_n s+1} \nmid (n!)$. Hence, we have a contradiction. We deduce that $(* * *)$ holds for some $v \in \{1, 2, \ldots, n\}$. Fix such a v. Since

$$h_v < \frac{v}{p} + \frac{v}{p^2} + \cdots = \frac{v}{p-1},$$

we deduce that

$$v \leq rv \leq h_v s < \frac{vs}{p-1} \leq \frac{vk}{p-1}.$$

Thus, $p - 1 < k$ so that $p < k + 1$. We deduce that $p \leq k$, as desired. ■