Introduction to Extensions of $\mathbb{Q}$

What makes work with rational numbers and integers comfortable are the essential properties they have, especially the unique factorization property (the Main Theorem of Arithmetic). However, the might of the arithmetic in $\mathbb{Q}$ is bounded. Thus, some polynomials, although they have zeros, cannot be factorized into polynomials with rational coefficients. Nevertheless, such polynomials can always be factorized in a wider field. For instance, the polynomial x^2+1 is irreducible over $\mathbb{Z}$ or $\mathbb{Q}$, but over the ring of the so called *Gaussian integers* $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ it can be factorized as $(x+i)(x-i)$. Sometimes the wider field retains many properties of the rational numbers. In particular, it will turn out that the Gaussian integers are a unique factorization domain, just like the (rational) integers $\mathbb{Z}$. We shall first discuss some basics of higher algebra.

Definition

A number $\alpha\in\mathbb{C}$ is *algebraic* if there is a polynomial $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ with integer coefficients such that $p(\alpha)=0$. If $a_n=1$, then α is an *algebraic integer*.

Further, $p(x)$ is the *minimal polynomial* of α if it is irreducible over $\mathbb{Z}[x]$ (i.e. it cannot be written as a product of nonconstant polynomials with integer coefficients).

Example 1

The number i is an algebraic integer, as it is a root of the polynomial x^2+1 which is also its minimal polynomial. Number $\sqrt{2}+\sqrt{3}$ is also an algebraic integer with the minimal polynomial x^4-10x^2+1 (verify!).

Example 2

The minimal polynomial of a rational number $q=a/b$ ($a\in\mathbb{Z}$, $b\in\mathbb{N}$, $(a,b)=1$) is $bx-a$. By the definition, q is an algebraic integer if and only if $b=1$, i.e. if and only if q is an integer.

Definition

Let α be an algebraic integer and $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ($a_i \in \mathbb{Z}$) be its minimal polynomial. The *extension* of a ring A by the element α is the set $A[\alpha]$ of all complex numbers of the form

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \ \ (c_i \in A), \qquad (*)$$

with all the operations inherited from A. The *degree* of the extension is the degree n of the polynomial $p(x)$.

The theme of this text are extensions of the ring $\mathbb{Z}$ of degree 2, so called *quadratic extensions*. Thus, for example, the polynomials $x^2 + 1$ and $x^2 + x + 1$ determine the extensions $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ (this notation will be used later).

All elements of a quadratic extension of $\mathbb{Z}$ are algebraic integers with the minimal polynomial of second degree. Two elements having the same minimal polynomials are said to be *conjugates*. Each nonrational element z of the quadratic extension has exactly one conjugate, called the conjugate of z and denoted $\overline{z}$. For a rational integer z we define $\overline{z} = z$.

Definition

The *norm* of an element z of a quadratic extension of $\mathbb{Z}$ is $N(z) = z\overline{z}$.

The norm is always an integer. Roughly speaking, it is a kind of equivalent of the absolute value in the set of integers $\mathbb{Z}$.

Example 3

If $z \in \mathbb{Z}[\sqrt{d}]$, $z = a + b\sqrt{d}$ ($a, b \in \mathbb{Z}$), then $\overline{z} = a - b\sqrt{d}$ and $N(z) = a^2 - db^2$. In particular, in $\mathbb{Z}[i]$ the norm of element $a + bi$ ($a, b \in \mathbb{N}$) is $N(a + bi) = a^2 + b^2$.

If $z = a + b\omega \in \mathbb{Z}[\omega]$ ($a, b \in \mathbb{Z}$), then $\overline{z} = a - b - b\omega$ and $N(z) = a^2 - ab + b^2$.

In every complex quadratic field the conjugation corresponds to the complex conjugation.

The following two propositions follow directly from definition.

Theorem 1

The conjugation is multiplicative, i.e. for arbitrary elements z_1, z_2 of a quadratic extension of $\mathbb{Z}$ it holds that $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$. □

Theorem 2

The norm is multiplicative, i.e. for arbitrary elements z_1, z_2 of a quadratic extension of $\mathbb{Z}$ it holds that $N(z_1 z_2) = N(z_1)N(z_2)$.

An element $\epsilon \in \mathbb{Z}[\alpha]$ is called a *unit* if there exists $\epsilon' \in \mathbb{Z}[\alpha]$ such that $\epsilon\epsilon' = 1$. In that case $N(\epsilon)N(\epsilon') = N(1) = 1$, so $N(\epsilon) = \pm 1$. In fact, ϵ is a unit if and only if its norm is ± 1: indeed, if $N(\epsilon) = \pm 1$ then $\epsilon\bar{\epsilon} = \pm 1$ by definition.

Example 4

The only units in $\mathbb{Z}$ are ± 1.

Let us find the units in $\mathbb{Z}[i]$. If $a + bi$ ($a, b \in \mathbb{Z}$) is a unit, then $N(a + bi) = a^2 + b^2 = \pm 1$, which implies $a + bi \in \{\pm 1, \pm i\}$.

All units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm(1 + \omega)$. Indeed, if $a + b\omega$ is a unit then $a^2 - ab + b^2 = 1$, i.e. $(2a - b)^2 + 3b^2 = 4$ and he result follows. Note that ω^2 equals $-(1 + \omega)$.

Problem 1

Let p be a prime number and $N = \prod_{k=1}^{p-1}(k^2 + 1)$. Determine the remainder of N upon division by p.

Hide solution

Denote $P(x) = (1 + x)(2 + x)\ldots(p - 1 + x)$. We know that $P(x) = x^{p-1} - 1 + pQ(x)$ for some polynomial $Q(x)$ with integer coefficients.

Since $k^2 + 1 = (k + i)(k - i)$ for each k, we immediately obtain that

$$N = P(i)P(-i) = \left(i^{p-1} - 1 + pQ(i)\right)\left((-i)^{p-1} - 1 + pQ(-i)\right)$$

$$\equiv \begin{cases} 4, & \text{if } p \equiv 3 \pmod 4; \\ 0, & \text{otherwise.} \end{cases}$$

The divisibility and congruences in an extension K of the ring $\mathbb{Z}$ is defined in the usual way: $x \in K$ is divisible by $y \in K$ (denoted $y \mid x$) if there exists $z \in K$ such that $x = yz$, and $x \equiv y \pmod z$ if $z \mid x - y$.

Since every element of a quadratic ring is divisible by every unit, the definition of the notion of a prime must be adjusted to the new circumstances.

Definition

An element y of a quadratic ring K is *adjoint* to element x (denoted $y \sim x$) if there exists a unit ϵ such that $y = \epsilon x$.

Definition

A nonzero element $x \in K$ which is not a unit is *prime* if it has no other divisors but the units and elements adjoint to itself.

We have the following simple proposition.

Theorem 3

Let $x \in K$. If $N(x)$ is a prime, then x is prime.

Hide proof

Suppose that $x = yz$, $y, z \in K$. Then $N(x) = N(y)N(z)$, so at least one of $N(y), N(z)$ equals ± 1, i.e. either y or z is a unit, while the other is (by definition) adjoint to x.

The converse does not hold, as 3 is a prime in $\mathbb{Z}[i]$, but $N(3) = 9$ is composite.

Of course, the elements conjugate or adjoint to a prime are also primes. Therefore the smallest positive rational integer divisible by a prime z equals $z\bar{z} = N(z)$.

Consider an arbitrary nonzero and nonunit element $x \in K$. If x is not prime then there are nonunit elements $y, z \in K$ such that $yz = x$. Hereby $N(y)N(z) = N(x)$ and $N(y), N(z) > 1$. Hence $N(y), N(z) < N(x)$. Continuing this procedure we end up with a factorization $x = x_1 x_2 \cdots x_k$ in which all elements are prime. This shows that:

Theorem 4

Every nonzero and nonunit $x \in K$ can be factorized into primes.

Problem 2

Given a nonzero and nonunit element $z \in K$, find the number of equivalence classes in K modulo z.

Hide solution

Let $K = \mathbb{Z}[\alpha]$, where $\alpha^2 = p\alpha + q$, $p, q \in \mathbb{Z}$, and let $z = a + b\alpha$ ($a, b \in \mathbb{Z}$). If $b = 0$ then $a_1 + b_1\alpha \equiv a_2 + b_2\alpha$ (mod z) if and only if $a_1 \equiv a_2$ and $b_1 \equiv b_2$ (mod z). Thus there are $N(z) = z^2$ equivalence classes.

Now suppose that $b \neq 0$ and that $(a, b) = d$. Then $\alpha z = (a + pb)\alpha + qb$. Since $(a + pb, b) = d$, the coefficient at α in xz ($x \in K$) can be any integer divisible by d and no other integer. Moreover, the smallest natural number divisible by z is $|(a + b\alpha)(\overline{a + b\alpha})|/d = |N(z)|/d$. We conclude that for every $x \in K$ there is a unique $X = A + B\alpha \in K$ with $A, B \in \mathbb{Z}$,

$0 \leq A < |N(z)|/d$, $0 \leq B < d$ such that $x \equiv X$ (mod z). Therefore the required number of equivalence classes equals $|N(z)|$.

Naturally, we would like to know when the factorization into primes is unique, i.e. when the Fundamental Theorem of Arithmetic holds. But let us first note that, by the above definition, the primes of $\mathbb{Z}$ are $\pm 2, \pm 3, \pm 5$, etc, so the factorization into primes is not exactly unique, as e.g. $2 \cdot 3 = (-2)(-3)$. Actually, in this case the uniqueness of factorization is true in the following wording.

Definition

FTA, or "The Fundamental Theorem of Arithmetic" means: Each nonzero and nonunit element of $\mathbb{Z}$ or of its quadratic extension K can be written as a product of primes. This factorization is unique up to the order of the factors and adjoining between corresponding factors.

The division with remainder in a quadratic extension K of $\mathbb{Z}$ can be formulated as follows:

Definition

DWR means: For each $a, b \in K$ with $b \neq 0$ there exist $p, q \in K$ such that $a = pb + q$ and $N(q) < N(b)$.

Obviously, such a division, if it exists, is not necessarily unique - it is not so even in $\mathbb{Z}$ itself. Moreover, it does not exist in some quadratic extensions, as we shall see later. The significance of the existence of a division with remainder, however, lies in the fact that it implies the uniqueness of factorization:

Theorem 5

If the division with remainder in a quadratic ring K is always possible, then FTA holds in K.

Hide proof

If the division with remainder is possible in K, then the Euclidean algorithm ends in a finite number of steps. A simple implication of the Euclidean algorithm is that if p is a prime, $a, b \in K$ and $p \mid ab$, then $p \mid a$ or $p \mid b$. The uniqueness of factorization into primes (FTA) now easily follows.

There are quadratic rings in which FTA holds despite the nonexistence of a division with remainder. However, FTA is an exception rather than a rule.

Example 5

FTA is false in $\mathbb{Z}[\sqrt{-5}]$, as 9 has two factorizations into primes:
$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, which are not equivalent since
$2 \pm \sqrt{-5} \nsim 3$.

Example 6

The factorizations of the element $4-\omega$ in $\mathbb{Z}[\omega]$ as
$(1-\omega)(3+\omega) = (-2-3\omega)(1+2\omega)$ are considered the same, since
$1+2\omega = \omega(1-\omega) \sim 1-\omega$ and $-2-3\omega = -(1+\omega)(3+\omega) \sim 3+\omega$.
We shall show later that FTA is true in $\mathbb{Z}[\omega]$.

Arithmetics in extensions of $\mathbb{Q}$ (Table of contents)

Arithmetics in Gaussian Integers $\mathbb{Z}[i]$

We have already seen that the norm of element $a+bi \in \mathbb{Z}[i]$ $(a,b \in \mathbb{Z})$ is $N(a+bi)=a^2+b^2$ and the units are ± 1 and $\pm i$. Therefore, all divisors of a prime element $\pi \in \mathbb{Z}[i]$ are $\pm 1, \pm i, \pm \pi, \pm i\pi$.

Theorem 6

The Fundamental Theorem of Arithmetic (FTA) holds in the set of Gaussian integers $\mathbb{Z}[i]$.

Hide proof

Based on theorem 5, it is enough to show that for all $a,b \in \mathbb{Z}[i]$ with $b \neq 0$ there exists an element $p \in \mathbb{Z}[i]$ such that $N(a-pb) < N(b)$.

Let $\sigma, \tau \in \mathbb{R}$ be such that $a/b = \sigma + \tau i$, and let $s,t \in \mathbb{Z}$ be such that $|\sigma - s| \leq 1/2$ and $|\tau - t| \leq 1/2$. Setting $p = s+ti$ yields $a-pb = (\sigma+\tau i)b - pb = [(\sigma - s) + (\tau - t)i]b$, which implies

$$N(a-pb) = N[(\sigma-s)+(\tau-t)i]N(b) = [(\sigma-s)^2+(\tau-t)^2]N(b) \leq N(b)/2 < N(b).$$

This proves the theorem.

The following proposition describes all prime elements in the set of Gaussian integers.

Theorem 7

An element $x \in \mathbb{Z}[i]$ is prime if and only if $N(x)$ is a prime or $|x|$ is a prime integer of the form $4k-1$, $k \in \mathbb{N}$.

Hide proof

Consider an arbitrary prime $x = a+bi \in \mathbb{Z}[i]$ $(a,b \in \mathbb{Z})$. Element $\overline{x}$ is prime also (indeed, if $\overline{x} = yz$, then $x = \overline{y}\,\overline{z}$), so $N(x)$ factorizes into primes as $x\overline{x}$.

Suppose that $N(x)$ is composite, $N(x) = mn$ for some two natural numbers $m,n>1$. It follows from $x\overline{x} = mn$ and the FTA that $x \sim m$ or $x \sim n$, so we may suppose w.l.o.g. that x is a prime integer. If $x = 2$ or $x \equiv 1$ (mod 4), then there exist integers $a,b \in \mathbb{Z}$ such that $N(a+bi) = (a+bi)(a-bi) = a^2+b^2 = x$; hence x is composite in $\mathbb{Z}[i]$. On the other hand, if x is a prime integer with $x \equiv 3$ {\rm(mod 4)}, then x is also prime in $\mathbb{Z}[i]$. Indeed, if $x = uv$ for some nonunit elements $u,v \in \mathbb{Z}[i]$, then $x^2 = N(x) = N(u)N(v)$ implies $N(u) = N(v) = x$ which is impossible. This proves our claim.

Problem 3

Solve the equation $x^5 - 1 = y^2$ in integers.

Hide solution

Rewrite the equation in the form $x^5 = (y+i)(y-i)$. Note that x is not even, as otherwise $y^2 \equiv -1 \pmod 4$. Thus y is even and consequently the elements $y+i$ and $y-i$ are coprime in $\mathbb{Z}[i]$. Since $(y+i)(y-i)$ is a fifth power, it follows that $y+i$ and $y-i$ are both fifth powers. Let $a, b \in \mathbb{Z}$ be such that
$y+i = (a+bi)^5 = a(a^4 - 10a^2b^2 + 5b^4) + b(5a^4 - 10a^2b^2 + b^4)i$. It holds that $b(5a^4 - 10a^2b^2 + b^4) = 1$, and therefore $b = \pm 1$. It is easily seen that we must have $y = 0$ and $x = 1$.

Problem 4

Suppose that x, y and z are natural numbers satisfying $xy = z^2 + 1$. Prove that there exist integers a, b, c, d such that $x = a^2 + b^2$, $y = c^2 + d^2$ and $z = ac + bd$.

Hide solution

We use the following important fact: If m, n, p, q are elements of a unique factorization domain K (in this case, $K = \mathbb{Z}[i]$) satisfying $mn = pq$, then there exist $u_1, u_2, v_1, v_2 \in K$ such that $m = u_1v_1$, $n = u_2v_2$, $p = u_1v_2$, $q = u_2v_1$. The proof of this fact is the same as in the case of $m, n, p, q \in \mathbb{Z}$ and follows directly from the factorizations of m, n, p, q into primes.

Since $xy = z^2 + 1 = (z+i)(z-i)$, the above fact gives us

$$x = u_1v_1 \quad (1), \quad y = u_2v_2 \quad (2), \quad z + i = u_1v_2 \quad (3), \quad z - i = u_2v_1 \quad (4)$$

for some $u_1, u_2, v_1, v_2 \in \mathbb{Z}[i]$. The numbers x, y are real, and therefore $v_1 = q_1\overline{u_1}$, $v_2 = q_2\overline{u_2}$ for some rational numbers q_1, q_2. From (3) and (4) we easily conclude that $q_1 = q_2 = 1$. Now putting $u_1 = a + bi$, $u_2 = c + di$ yields $x = u_1\overline{u_1} = a^2 + b^2$, $y = c^2 + d^2$ and $z = ac + bd$.

Arithmetics in extensions of $\mathbb{Q}$ (Table of contents)

Arithmetics in the ring $\mathbb{Z}[\omega]$

Here ω denotes a primitive cubic root of unity. Then the norm of an element $a+b\omega \in \mathbb{Z}[\omega]$ ($a,b \in \mathbb{Z}$) is $N(a+b\omega) = a^2 - ab + b^2$ and the units are ± 1, $\pm\omega$ and $\pm(1+\omega) = \mp\omega^2$.

Theorem 8

FTA holds in the ring $\mathbb{Z}[\omega]$.

Hide proof

By the theorem 5, it suffices to show that a division with remainder is possible, i.e. for all $a, b \in \mathbb{Z}[\omega]$, $b \neq 0$ there exist $p \in \mathbb{Z}[\omega]$ such that $N(a-pb) < N(b)$.

Like in the proof for the Gaussian integers, let $\sigma, \tau \in \mathbb{R}$ be such that $a/b = \sigma + \tau i$, and let $s, t \in \mathbb{Z}$ be such that $|\sigma - s| \leq 1/2$ and $|\tau - t| \leq 1/2$. Setting $p = s + ti$ gives us $N(a-pb) \leq 3N(b)/4 < N(b)$, implying the theorem.

Problem 5

If $p \equiv 1 \pmod 6$ is a prime number, prove that there exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.

Hide solution

It suffices to show that p is composite in $\mathbb{Z}[\omega]$. Indeed, if there is a prime element $z = a + b\omega \in \mathbb{Z}[\omega]$ ($a, b \in \mathbb{Z}$) that divides p, then also $\overline{z} \mid \overline{p} = p$. Note that z and $\overline{z}$ are coprime; otherwise $z \mid \overline{z}$, so there exists a unit element ϵ with $\overline{z} = \epsilon z$, and hence $z \sim (1-\omega) \mid 3$, which is false. Therefore $a^2 - ab + b^2 = z\overline{z} \mid p$, which implies $a^2 - ab + b^2 = p$.

Thus we need to prove that p is composite in $\mathbb{Z}[\omega]$. It follows from the condition on p that -3 is a quadratic residue modulo p, so there exist $m, n \in \mathbb{Z}$ which are not divisible by p such that $p \mid (2m-n)^2 + 3n^2 = 4(m^2 - mn + n^2)$, i.e. $p \mid (m - n\omega)\overline{m - n\omega}$. However, p does not divide any of the elements $(m - n\omega), \overline{m - n\omega}$, so it must be composite.

Theorem 9

Element $x \in \mathbb{Z}[\omega]$ is prime if and only if $N(x)$ is prime or $|x|$ is a prime integer of the form $3k-1$, $k \in \mathbb{N}$.

Hide proof

Number $x = 3$ is composite, as $N(1-\omega) = (1-\omega)(2+\omega) = 3$. Moreover, by problem 4, every prime integer $p \equiv 1 \pmod 6$ is composite in $\mathbb{Z}[\omega]$.

The rest of the proof is similar to the proof of Theorem 7 and is left as an exercise.

Maybe the most famous application of the elementary arithmetic of the ring $\mathbb{Z}[\omega]$ is the Last Fermat Theorem for the exponent $n = 3$. This is not unexpected, having in mind that $x^3 + y^3$ factorizes over $\mathbb{Z}[\omega]$ into linear factors:

$$x^3 + y^3 = (x+y)(x+\omega y)(x+\omega^2 y) = (x+y)(\omega x + \omega^2 y)(\omega^2 x + \omega y). \qquad (1)$$

The proof we present was first given by Gauss.

Theorem 10

The equation

$$x^3 + y^3 = z^3 \qquad (*)$$

has no nontrivial solutions in $\mathbb{Z}[\omega]$, and consequently has none in $\mathbb{Z}$ either.

Hide proof

Suppose that x, y, z are nonzero elements of $\mathbb{Z}[\omega]$ that satisfy $(*)$. We can assume w.l.o.g. that x, y, z are pairwise coprime.

Consider the number $\rho = 1 - \omega$. It is prime, as its norm equals $(1-\omega)(1-\omega^2) = 3$. We observe that $\overline{\rho} = 1 - \omega^2 = (1-\omega)(1+\omega) \sim \rho$; hence $\alpha \in \mathbb{Z}[\omega]$ is divisible by ρ if and only if so is $\overline{alpha}$. Each element in $\mathbb{Z}[\omega]$ is congruent to $-1, 0$ or 1 (mod ρ): indeed, $a + b\omega \equiv a + b = 3q + r \equiv r$ (mod ρ) for some $q \in \mathbb{Z}$ and $r \in \{-1, 0, 1\}$.

The importance of number ρ lies in the following property:

$$\alpha \equiv \pm 1 \pmod{\rho} \ (\alpha \in \mathbb{Z}[\omega]) \ \text{ implies } \ \alpha^3 \equiv \pm 1 \pmod{\rho^4}. \qquad (2)$$

Indeed, if $\alpha = \pm 1 + \beta\rho$, we have
$a^3 \mp 1 = (a \mp 1)(a \mp \omega)(a \mp \omega^2) = \rho^3\beta(\beta \pm 1)(\beta \pm (1+\omega))$, where the elements b, $b \pm 1$, $b \pm (1+\omega)$ leave three distinct remainders modulo ρ, implying that one of them is also divisible by ρ, thus justifying our claim.

Among the numbers x, y, z, (exactly) one must be divisible by ρ: otherwise, by (2), x^3, y^3, z^3 would be congruent to ± 1 (mod ρ^4), which would imply one of the false congruences $0 \equiv \pm 1$, $\pm 1 \equiv \pm 2$ (mod ρ^4). We assume w.l.o.g. that $\rho \mid z$. Moreover, (2) also gives us that $\rho^2 \mid z$.

Let $k \geq 2$ be the smallest natural number for which there exists a solution to $(*)$ with $(x, y, z) = 1$ and $\rho^k \mid z$, $\rho^{k+1} \nmid z$. Consider this solution (x, y, z).

The factors $x+y$, $\omega x+\omega^2 y$, $\omega^2 x+\omega y$ from (1) are congruent modulo ρ and have the sum 0. It follows from $\rho \mid z$ that each of them is divisible by ρ and that ρ is their greatest common divisor. Let

$$x+y=A\rho, \quad \omega x+\omega^2 y=B\rho, \quad \omega^2 x+\omega y=C\rho,$$

where $A, B, C \in \mathbb{Z}[\omega]$ are pairwise coprime and $A+B+C=0$. The product ABC is a perfect cube (equal to $(z/\rho)^3$), and hence each of A, B, C is adjoint to a cube:

$$A=\alpha\zeta^3, \quad B=\beta\eta^3, \quad C=\gamma\xi^3$$

for some pairwise coprime $\zeta, \eta, \xi \in \mathbb{Z}[\omega]$ and units α, β, γ. Therefore,

$$\alpha\zeta^3+\beta\eta^3+\gamma\xi^3=0. \qquad (3)$$

Since $\alpha\beta\gamma$ is a unit and a perfect cube, we have $\alpha\beta\gamma=\pm 1$. Furthermore, $ABC=(z/\rho)^3$ is divisible by ρ (since $\rho^2 \mid z$), so (exactly) one of the numbers ζ, η, ξ, say ξ, is divisible by ρ. In fact, ξ^3 divides ABC which is divisible by ρ^{3k-3} and not by ρ^{3k-2}, so ρ^{k-1} is the greatest power of ρ that divides ξ. The numbers ζ and η are not divisible by ρ; consequently, ζ^3 and η^3 are congruent to ± 1 modulo ρ^4. Thus the equality $A+B+C=0$ gives us $\alpha \pm \beta \equiv 0 \pmod{\rho^4}$, therefore $\beta=\pm\alpha$; now $\alpha\beta\gamma=\pm 1$ implies $\gamma=\pm\alpha$.

Canceling α in equation (3) yields $\zeta^3 \pm \eta^3 \pm \xi^3=0$, which gives us another nontrivial solution to $(*)$ with $(\zeta, \eta, \xi)=1$. However, in this solution we have $\rho^{k-1} \mid \xi$ and $\rho^k \nmid \xi$, which contradicts the choice of k.

Arithmetics in extensions of $\mathbb{Q}$ (Table of contents)

Arithmetics in Other Quadratic Rings

Every quadratic ring belongs to one of the two classes:

- 1° Extensions of the form $K = \mathbb{Z}[\sqrt{d}]$, where $d \neq 1$ is a squarefree integer. The conjugation and norm are given by the formulas $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$ and $N(x + y\sqrt{d}) = x^2 - dy^2$, where $x, y \in \mathbb{Z}$.

- 2° Extensions of the form $K = \mathbb{Z}[\alpha]$ for $\alpha = \frac{-1+\sqrt{d}}{2}$, where $d = 4k + 1$ ($k \in \mathbb{Z}$) is a squarefree integer with $d \neq 1$ (then α is an algebraic integer: $\alpha^2 + \alpha - k = 0$). The conjugation and norm are given by $\overline{x + y\alpha} = x - y - y\alpha$ and $N(x + y\alpha) = x^2 - xy - ky^2$, where $x, y \in \mathbb{Z}$.

  Some of these rings are Euclidean, such as $\mathbb{Z}[\sqrt{d}]$ for $d = -2, -1, 2, 3, 6, 7$ and $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ for $d = -7, -3, 5$.

Determining all quadratic unique factorization rings (including the non-Euclidean ones) is extremely serious. Among the rings of the type 1° and 2° with $d < 0$, apart from the ones mentioned already, the FTA holds in only five other rings: namely, the rings of the type 2° for $d = -11, -19, -43, -67, -163$. Gauss' conjecture that the FTA holds in infinitely many quadratic rings with a positive d has not been proved nor disproved until today.

Problem 6

Find all integer solutions of the equation $x^2 + 2 = y^3$.

Hide solution

Let us write the equation as $(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$. For x even we have $y^3 \equiv 2 \pmod 4$, which is impossible; therefore x is odd. Then $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are coprime elements of $\mathbb{Z}[\sqrt{-2}]$ whose product is a perfect cube. Using the FTA in $\mathbb{Z}[\sqrt{-2}]$ we conclude that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are both perfect cubes. Hence there exist $a, b \in \mathbb{Z}$ such that $(a + b\sqrt{-2})^3 = x + \sqrt{-2}$. Comparing the coefficients at $\sqrt{-2}$ yields $b(3a^2 - 2b^2) = 1$; therefore $b = 1$ and $a = \pm 1$. Now we easily obtain that $x = \pm 5$ and $y = 3$ is the only integral solution of the equation.

Problem 7

Consider the sequence $a_0, a_1, a_2, \ldots$ given by $a_0 = 2$ and $a_{k+1} = 2a_k^2 - 1$ for $k \geq 0$. Prove that if an odd prime number p divides a_n, then $p \equiv \pm 1 \pmod{2^{n+2}}$.

Hide solution

Consider the sequence x_k of positive numbers given by $a_k = \cosh x_k$ ($\cosh$ is the *hyperbolic cosine*, defined by $\cosh t = \frac{e^t + e^{-t}}{2}$). It is easily verified that $\cosh(2x_k) = 2a_k^2 - 1 = \cosh x_{k+1}$, so $x_{k+1} = 2x_k$, i.e. $x_k = \lambda \cdot 2^k$ for some $\lambda > 0$. The condition $a_0 = 2$ gives us $\lambda = \log(2 + \sqrt{3})$. Therefore

$$a_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}.$$

Let $p > 2$ be a prime number such $p \mid a_n$. We distinguish two cases.

- 1° $m^2 \equiv 3 \pmod{p}$ for some $m \in \mathbb{Z}$. Then

  $$(2+m)^{2^n} + (2-m)^{2^n} \equiv 0 \pmod{p}. \qquad (1)$$

  Since $(2+m)(2-m) = 4 - m^2 \equiv 1 \pmod{p}$, multiplying both sides of (1) by $(2+m)^{2^n}$ yields $(2+m)^{2^{n+1}} \equiv -1 \pmod{p}$. It follows that the order of number $(2+m)$ modulo p equals 2^{n+2}, from which we conclude $2^{n+2} \mid p - 1$.

- 2° The congruence $m^2 \equiv 3 \pmod{p}$ has no solutions. We work in the quadratic extension $\mathbb{Z}_p(\sqrt{3})$ of the field $\mathbb{Z}_p$ in which number $\sqrt{3}$ actually plays the role of the number m from case (1). As in case (1) we have $(2+\sqrt{3})^{2^{n+1}} = -1$, which means that the order of $2 + \sqrt{3}$ in the multiplicative group $\mathbb{Z}_p(\sqrt{3})^*$ equals 2^{n+2}. This is not enough to finish the proof as in case (1), as the group $\mathbb{Z}_p(\sqrt{3})^*$ has $p^2 - 1$ elements; instead, we only get that $2^{n+2} \mid p^2 - 1$. However, we shall be done if we find $u \in \mathbb{Z}_p(\sqrt{3})$ for which $u^2 = 2 + \sqrt{3}$: indeed, then the order of u is 2^{n+3}, so $2^{n+3} \mid p^2 - 1$ and therefore $2^{n+2} \mid p - 1$, since $4 \nmid p + 1$.

  Note that $(1+\sqrt{3})^2 = 2(2+\sqrt{3})$. Now it is enough to show that $1/2$ is a perfect square in the field $\mathbb{Z}_p(\sqrt{3})$. This immediately follows from the relation $a_n = 0 = 2a_{n-1}^2 - 1$, as $1/2 = a_{n-1}^2$. This finishes the proof.

Arithmetics in extensions of $\mathbb{Q}$ (Table of contents)