Lecture Notes On Abstract Algebra (Week 5)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

October 7, 2023

Contents

1 A Brief History of Commutative Rings

The theory of commutative rings (that is rings in which multiplication is commutative) and the theory of non-commutative rings were studied quite independently of each other until about 1930 and as traces of the commutative theory appear first it is with this theory that we begin.

The study of a ring provided a generalization of integer arithmetic is the clue to the early development of commutative ring theory. For example Legendre and Gauss investigated integer congruences in 1801. However, the motivation for generalizing arithmetic came mostly from attempts-to prove *Fermat's Last Theorem*. This theorem, proved as recently as 1995 by A. wiles and R. Taylor, states that the equation

$$x^n + y^n = z^n$$

has no solution for positive integers x, y, z when $n > 2$.

This statement, thought to have been made in the late 1630's, was found in the marginal notes that Fermat had made in Bachet's translation of *Diophantus's Arithmetica*.

Attempts to prove this result led to proofs in the following special cases:

- $n = 4$, Fermat, about 1640
- $n = 3$, Euler, 1753
- $n = 5$, Legendre and Dirichlet, 1825
- $n = 7$, Lamé, 1839; Lebesgue, 1840

Euler's work on the case $n = 3$ involved extending ordinary integer arithmetic to apply to the ring $\mathbb{Z}[\sqrt{-3}]$ of numbers of the form $a + b\sqrt{-3}$ where a, b are integers. However, Euler failed to grasp the difficulties of working in this ring and made certain assertions which, although true, would be hard to justify. In 1847 Lamé announced that he had a solution of Fermat's Last Theorem and sketched out a proof. Liouville suggested that the proof depended on a unique decomposition into primes which was unlikely to be true. However, Cauchy supported Lamé. The argument which followed indicates the totally different atmosphere surrounding mathematical research of this period from that which we know today. Perhaps we could illustrate the point causing this argument. Complex numbers of the form $a + b\sqrt{-3}$, where a, b are integers, form a ring. A prime number in this ring is defined in an analogous way to a prime integer, namely a number whose only divisors of the form $a + b\sqrt{-3}$ other than itself are those numbers with multiplicative inverses. In this ring 4 can be written as a product of prime numbers in two different ways

$$4 = 2 \times 2 \text{ and } 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Gauss had proved around 1801 that numbers of the form $a + b\sqrt{-1}$, where a, b are integers, could be written uniquely as a product of prime numbers of the form $a + b\sqrt{-1}$ in an analogous manner to the unique decomposition of an integer as a product of prime integers. In fact, numbers of the form $a + b\omega + c\omega^2$ where a, b, c are integers and $\omega = \frac{-1+\sqrt{-3}}{2}$ is a complex cube root of 1, also have unique factorization, and this can be used to prove the $n = 3$ case of Fermat's last Theorem.

The argument following Lamé's announcement was settled by Kummer who pointed out that he had published an example in 1844 to show that the uniqueness of such decompositions failed and in 1846 he had restored the uniqueness by introducing "ideal complex numbers". He then saw the relevance of his theory to Fermat's Last Theorem. The popular story that Kummer invented "ideal complex numbers" in an attempt to correct an error in this proof of Fermat's Last Theorem is almost certainly false. In 1847, just after Lamé's announcement, Kummer used his "ideal complex numbers" to prove Fermat's Last Theorem for all $n < 100$ except $n = 37, 59, 67$ and 74.

Up to this point we are still firmly within the realms of number theory but the genius of Dedekind pinpointed the important properties of the "ideal complex numbers". Dedekind defined an "ideal", characterizing it by its now familiar properties: namely that of being an additive subgroup whose elements, on being multiplied by any ring element, remain in the subgroup. Ring theory in its own right was born together with an early hint of the axiomatic method which was to dominate algebra in the 20thCentury. Dedekind also introduced the word "module" in 1871 although its initial definition was considerably more restricted than the present definition, being first introduced as a subgroup of the additive group of a ring; the term is now used for a "vector space with coefficients from a ring".

Prime numbers were generalized to prime ideals by Dedekind in 1871. A prime ideal is an ideal which contains the product of two elements only if it contains one of the two elements. For example all integers divisible by a fixed prime p form a prime ideal of the ring of integers. This trend towards looking at ideals rather than elements marks an important stage in the development of ring theory.

In 1882 an important paper by Dedekind and Weber accomplished two things; it related geometric ideas with rings of polynomials and extended the use of modules. It is important to realize that at this stage rings of polynomials and rings of numbers were being studied, but it was to be another 40 years before an axiomatic theory of commutative rings was to be developed bringing these theories together.

Although the concept of a ring is due to Dedekind, one of the first words used was an "order". This term, invented by Kronecker, is still used today in algebraic number theory. Dedekind did introduce the term "field" (Körper) for a commutative ring in which every non-zero element has a multiplicative inverse but the word "number ring" (Zahlring) or "ring" is due to Hilbert. Hilbert, motivated by studying invariant theory, studied ideals in polynomial rings proving his famous "Basis Theorem" in 1893. Special cases of this theorem had been studied by Gordan from 1868 and on seeing Hilbert's proof Gordan is said to have exclaimed "This is not mathematics, it's theology".

The decomposition of an integer into the product of powers of primes has an analogue in rings where prime integers are replaced by prime ideals but, rather surprisingly, powers of prime integers are not replaced by powers of prime ideals but rather by "primary ideals". Primary ideals were introduced in 1905 by Lasker in the context of polynomial rings. (Lasker was World Chess Champion from 1894 to 1921.) Lasker proved the existence of a decomposition of an ideal into primary ideals but the uniqueness properties of the decomposition were not proved until 1915 by Macaulay.

I. D. Macdonald notes in his article *Modern Algebra in the Nineteenth Century* (in Aust. Math. Teacher) that algebra texts in early years contained axioms for groups similar to many present-day texts. However, the axiomatic treatment of commutative rings was not developed until the 1920's in the work of Emmy Noether and Krull. Emmy Noether, one of the world's greatest women mathematicians, was a student of Gordan's. In about 1921 she made the important step, which we commented on earlier, of bringing the two theories of rings of polynomials and rings of numbers under a single theory of abstract commutative rings. Discrimination made it difficult for her to publish her work and it was not until Van der Waerden's important work on Modern Algebra was published in 1930 that Noether's results become widely known.

In contrast to commutative ring theory, which as we have seen grew from number theory, non-commutative ring theory developed from an idea which, at the time of its discovery, was heralded as a great advance in applied mathematics. Hamilton attempted to generalize the complex numbers as a two dimensional algebra over the reals to a three dimensional algebra. Hamilton, who introduced the idea of a vector space, felt that this three dimensional analogue of the complex numbers would revolutionize applied mathematics but he struggled unsuccessfully with the idea for many years. In 1843 inspiration struck Hamilton — the generalization was not to three dimensions but to four dimensions and the commutative property of multiplication no longer held. The quaternion algebra, as Hamilton called this four dimensional algebra, was widely used in applied mathematics (where it was later replaced by the vector product) and it launched non-commutative ring theory.

Matrices with their laws of addition and multiplication were introduced by Cayley in 1850 while, in 1870, Pierce noted that the now familiar ring axioms held for square matrices — another early example of the axiomatic approach to rings. The greatest early contributor to the theory of non-commutative rings was the Scottish mathematician Wedderburn. In 1905 he proved that every finite *division ring* (a ring in which every non-zero element has a multiplicative inverse) is commutative and so is a field. In 1908 Wedderburn had the important idea of splitting the study of a ring into two parts, one part he called the radical, the part which was left being called semi-simple. He used matrix rings to classify the semi-simple part. The importance of this work can be seen from the fact that the next 56 years were spent generalizing it. It should be pointed out that Wedderburn did not prove his results for rings but rather for hypercomplex systems — a term no longer in use which meant a finite dimensional algebra over a field.

The Wedderburn theory was extended to non-commutative rings satisfying both ascending and descending finiteness conditions (called chain conditions) by Artin in 1927. It was not until 1939 that Hopkins showed that only the descending chain condition was necessary.

Around the 1930's the theories of commutative and non-commutative rings came together and the ideas of one began to influence the other. For example, chain conditions in both commutative and non-commutative rings are investigated at much the same time. Modules, originally introduced for commutative rings, were studied for general rings. Some ideas, however, were slow to filter from one theory to the other, for example, prime ideals for non-commutative rings were not studied until 1949 by McCoy.

In the 1940's attempts were made to prove results of the Wedderburn-Artin type for rings without chain conditions. The breakthrough here was made in 1945 by Jacobson who was a student of Wedderburn's using ideas of Perlis in 1942. It is interesting to note that this fundamental work by Jacobson hinges on the idea of the "Jacobson radical" of a ring which is an analogue of a group theory idea due to Frattini as early as 1885.

2 A Special Case of Fermat's Last Theorem

Fermat's Last Theorem (sometimes called Fermat's Conjecture) states that no three positive integers x, y, and z can satisfy the equation

$$x^n + y^n = z^n$$

for any positive integer value of $n \geq 3$. It's clear that solving Fermat's Last Theorem reduces to the the case that $n = 4$ and n being an odd prime integer.

This theorem was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of *Arithmetica* where he claimed he had a proof that was too large to fit in the margin. The first successful proof was released in 1994 by Andrew Wiles and Richard Taylor, and formally published in 1995, after 358 years of effort by mathematicians. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem on elliptic curves over the rationals in the 20th century. It is among the most notable theorems in the history of mathematics and prior to its proof it was in the *Guinness Book of World Records* for "most difficult mathematical problems".

In this part we will prove a weaker result of Fermat's Last Theorem under the assumption that the domain $\mathbb{Z}[\zeta_p]$ has unique factorization property. Here ζ_p denotes a primitive p-th root of unity.

Theorem 2.1. *Let p be an odd prime and ζ_p a primitive p-th root of unity. Assume $\mathbb{Z}[\zeta_p]$ is a UFD. Then there is no integer solution (x, y, z) to the Fermat equation*

$$x^p + y^p = z^p \tag{1}$$

with $p \nmid xyz$.

Before giving out the proof, we need to understand more on the integral domain $\mathbb{Z}[\zeta_p]$. For simplicity, we write $\underline{R = \mathbb{Z}[\zeta_p] \text{ and } \zeta = \zeta_p}$.

Since $\zeta \in \mathbb{C}$ is algebraic and $x^{p-1} + x^{p-2} + \cdots + x + 1$ is the irreducible polynomial (minimal polynomial) of ζ, we have

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Hence

$$R = \mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots a_{p-2}\zeta^{p-2} \mid a_0, a_1, \cdots, a_{p-2} \in \mathbb{Z}\}$$

This means that for every $\alpha \in R$, there exist unique $a_0, a_1, \cdots, a_{p-2} \in \mathbb{Z}$ such that

$$\alpha = a_0 + a_1\zeta + \cdots a_{p-2}\zeta^{p-2}.$$

For $\alpha, \beta, \gamma \in R$, we use the notation $\alpha \equiv \beta (\text{mod } \gamma)$ to mean that $\gamma \mid \alpha - \beta$. This coincides with the same notation as in $\mathbb{Z}$. It's easy to check that the congruence symbol has the following property:

1. if $\alpha \equiv \beta (\text{mod } \gamma)$, $\alpha' \equiv \beta' (\text{mod } \gamma)$, then $\alpha\alpha' \equiv \beta\beta' (\text{mod } \gamma)$ and $\alpha \pm \alpha' \equiv \beta \pm \beta' (\text{mod } \gamma)$; In particular, $\alpha \equiv \beta (\text{mod } \gamma)$ implies $\alpha^n \equiv \beta^n (\text{mod } \gamma)$ for and $n \geq 0$;
2. if $\alpha \equiv \beta (\text{mod } \gamma)$, then $\overline{\alpha} \equiv \overline{\beta} (\text{mod } \overline{\gamma})$. Here $\overline{\alpha}$ denotes the complex conjugate of α.

Lemma 2.1. *Let $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in R$ and*

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \equiv 0 (\text{mod } n)$$

for some $n \in \mathbb{Z}$. Then $a_i \equiv 0 (\text{mod } n)$ for all $0 \leq i \leq p-2$.

Proof. Since $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \equiv 0 (\text{mod } n)$, we have

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} = n(b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2})$$

for some $b_0, b_1, \cdots, b_{p-2} \in \mathbb{Z}$. Let $f(t) = (a_0 - nb_0) + (a_1 - nb_1)t + \cdots + (a_{p-1} - nb_{p-2})t^{p-2}$. It follows $f(\zeta) = 0$. Note that $1 + t + \cdots + t^{p-1}$ is the irreducible polynomial of ζ. Then $1 + t + \cdots + t^{p-1} \mid f(t)$. So $f(t) = 0$. Consequently $a_i - nb_i = 0$ for all $0 \leq i \leq p-2$. It follows $a_i \equiv 0 (\text{mod } n)$ for all i. □

Lemma 2.2. *For $1 \leq i, j \leq p-1$, $\frac{1-\zeta^i}{1-\zeta^j} \in R^\times$. In particular, $1 - \zeta^i$ and $1 - \zeta$ are associates for $1 \leq i \leq p-1$.*

Proof. If $1 \leq i, j \leq p-1$, then $\gcd(i, p) = \gcd(j, p) = 1$. It follows from elementary number theory that there exist $a, b \in \mathbb{Z}$ such that $a > 0$ and $i = ja + pb$. Hence

$$1 - \zeta^i = 1 - \zeta^{ja+pb} = 1 - \zeta^{ja} = (1 - \zeta^j)(1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{(a-1)j}).$$

So

$$\frac{1-\zeta^i}{1-\zeta^j} = 1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{(a-1)j} \in R.$$

Similarly $\frac{1-\zeta^j}{1-\zeta^i} = \left(\frac{1-\zeta^i}{1-\zeta^j}\right)^{-1} \in R$. Thus we have $\frac{1-\zeta^i}{1-\zeta^j} \in R^\times$. □

Lemma 2.3. *The element $1 - \zeta$ is irreducible and $1 - \zeta \mid p$ in R.*

Proof. Note that the norm map $N : R \to \mathbb{Z}$ is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.

The roots of $t^p - 1$ are $1, \zeta, \cdots, \zeta^{p-1}$ and so

$$\frac{t^p - 1}{t - 1} = \prod_{i=1}^{p-1} (t - \zeta^i).$$

Hence

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i).$$

By Lemma 2.2, we have a unit $u \in R$ such that

$$p = (1 - \zeta)^{p-1} u. \tag{2}$$

Thus $1 - \zeta \mid p$ and $N(p) = p^{p-1} = \pm N(1 - \zeta)^{p-1}$, yielding $N(1 - \zeta) = p$. So $1 - \zeta$ is irreducible. □

We borrow a result from elementary number theory.

Proposition 2.1. *For $1 \le k \le p-1$, $\binom{p}{k} \equiv 0 (\mathrm{mod}\ p)$.*

Lemma 2.4. *For any $\alpha \in R$, there exist $a \in \mathbb{Z}$ such that $\alpha^p \equiv a (\mathrm{mod}\ p)$. In particular, if $\alpha \in \mathbb{Z}$ and $1-\zeta \mid \alpha$, then $p \mid \alpha$.*

Proof. For $\alpha \in R$, we have some $b \in \mathbb{Z}$ and $\beta \in R$ such that $\alpha = b + (1-\zeta)\beta$. Then

$$\alpha^p = b^p + (1-\zeta)^p \beta^p + \sum_{i=1}^{p-1} \binom{p}{i} b^{p-i} (1-\zeta)^i \beta^i.$$

Put $a = b^a$. Then it follows from Proposition and formula (2) that $\alpha^p \equiv a (\mathrm{mod}\ p)$.

If $\alpha \in \mathbb{Z}$ and $1-\zeta \mid \alpha$, then $(1-\zeta)^{p-1} \mid \alpha^{p-1}$. Hence $p \mid \alpha^p$ by formula (2). That is, $\alpha^p \equiv 0 (\mathrm{mod}\ p)$. But $\alpha^p \equiv \alpha (\mathrm{mod}\ p)$ (Fermat's Little Theorem). So $p \mid \alpha$. □

The following result is about the units of R. But we do not give out the proof. You may prove it as an exercise (not so easy!).

Lemma 2.5 (Kummer)**.** *For every $\alpha \in R^\times$, there exist $u \in \mathbb{R}$ such that*

$$\alpha = \zeta^r u$$

foe some $0 \le r \le p-1$.

For example, $\frac{1-\zeta_{19}^3}{1-\zeta_{19}^{12}} \in \mathbb{Z}[\zeta_{19}]^\times$ by Lemma 2.2. We have

$$\frac{1-\zeta_{19}^3}{1-\zeta_{19}^{12}} = \frac{1-\zeta_{19}^{22}}{1-\zeta_{19}^{12}} = \zeta_{19}^5 \cdot \frac{\zeta_{19}^{-11}-\zeta_{19}^{11}}{\zeta_{19}^{-6}-\zeta_{19}^{6}},$$

where

$$\frac{\zeta_{19}^{-11}-\zeta_{19}^{11}}{\zeta_{19}^{-6}-\zeta_{19}^{6}} = \frac{\sin\frac{22\pi}{19}}{\sin\frac{12\pi}{19}}$$

is a real unit.

Proof of Theorem 2.1

Let (x, y, z) be a solution of Fermat's equation (1) with $p \nmid xyz$. After removing any common factor, we may suppose that $\gcd(x, y, z) = 1$. Then x, y, z are pairwise relatively prime.

We first treat the case $p = 3$. The only cubes modulo 9 are $-1, 0, 1$, and so

$$x^3 + y^3 \equiv 2, 0, 2 (\mathrm{mod}\ 9), \quad z^3 \equiv -1, 1 (\mathrm{mod}\ 9),$$

which are contradictory. Similarly we may eliminate the case $p = 5$ by looking modulo 25. Henceforth we assume $p > 5$.

Note that $x^p + y^p + (-z)^p = 0$. If $x \equiv y \equiv -z \pmod{p}$, then $-2z^p \equiv z^p$ and $p \mid 3z$, contradicting with our hypotheses. Hence one of the congruences can't hold, and after rewriting the equation $x^p + (-z)^p = (-y)^p$ if necessary, we may assume that $p \nmid x - y$.

The roots of $t^p + 1$ are $-1, -\zeta, \cdots, -\zeta^{p-1}$ and so

$$t^p + 1 = \prod_{i=0}^{p-1} (t + \zeta^i).$$

Hence

$$\prod_{i=0}^{p-1}(x+\zeta^i y) = z^p. \tag{3}$$

The idea of the proof is to exploit this factorization and what we know of the arithmetic of $\mathbb{Z}(\zeta)$ to obtain a contradiction.

1. The elements $x+\zeta^i y$ of $\mathbb{Z}[\zeta]$ are pairwise relatively prime.

   Actually, if some irreducible element $\pi \mid (x+\zeta^i y)$ and $\pi \mid (x+\zeta^j y)$ for some $1 \le i < j \le p-1$, then $\pi \mid (1-\zeta^{j-i})y$ and $\pi \mid (1-\zeta^{j-i})x$. Note that $\gcd(x,y)=1$. Then $\pi \mid (1-\zeta^{j-i})$. By Lemma 2.2, we have $\pi \mid 1-\zeta$. This means π and $1-\zeta$ are associate. WLOG, we take $\pi = 1-\zeta$. It follows from $\pi \mid (x+\zeta^i y)$ that $x+y \equiv 0(\text{mod } 1-\zeta)$. But

   $$z^p = x^p + y^p = (x+y)^p - \sum_{k=1}^{p-1}\binom{p}{k}x^k y^{p-k}.$$

   So $z^p \equiv 0(\text{mod } 1-\zeta)$, yielding $z \equiv 0(\text{mod } 1-\zeta)$. This implies $p \mid z$ by Lemma 2.4, contradicting with our assumption on z.

2. Since R is a UFD, we have

   $$x+\zeta^i y = u_i\alpha_i^p \text{ for } 1 \le i \le p, \text{ and } \prod_{i=1}^{p}\alpha_i = z, \prod_{i=1}^{p}u_i = 1,$$

   where $u_i \in R^\times, \alpha_i \in R$.

   Take $i=1$, and put $u=u_1, \alpha=\alpha_1$. Then we have that

   $$x+\zeta y = u\alpha^p \tag{4}$$

   for some unit $u \in \mathbb{Z}[\zeta]$. We apply Lemma 2.5 to write $u = \zeta^r \cdot v$ where $\overline{v} = v$. According to Lemma 2.4, there is an $a \in \mathbb{Z}$ such that $\alpha^p \equiv a(\text{mod } p)$. Therefore

   $$x+\zeta y = \zeta^r v\alpha^p \equiv \zeta^r va(\text{mod } p)\text{and}$$
   $$x+\overline{\zeta}y \equiv \zeta^{-r}va(\text{mod } p).$$

   On combining these statements, we find that

   $$\zeta^{-r}(x+\zeta y) \equiv \zeta^r(x+\zeta^{-1}y)(\text{mod } p),$$

   or

   $$x+\zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0(\text{mod } p). \tag{5}$$

   If $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ are distinct, then Lemma 2.1 says $p \mid x$, which is contrary to our original assumption. So they are not distinct. The only remaining possibilities are that two of $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ are equal. There are essentially three cases: $1 = \zeta^{2r-1}, 1 = \zeta^{2r}$, $\zeta = \zeta^{2r-1}$.

   (a) $\zeta^{2r-1} = 1$; then $\zeta = \zeta^{2r}$, and (5) implies

   $$(x-y)(1-\zeta) \equiv 0(\text{mod } p),$$

   and hence $p \mid x-y$ by Lemma 2.4, which contradicts the choice of x and y made at the start of the first step of the proof.

(b) $\zeta^{2r} = 1$; but then (5) says

$$\zeta y - \zeta^{-1} y \equiv 0 (\text{mod } p),$$

and Lemma 2.4 implies $p \mid y$, which contradicts our original assumption.

(c) $\zeta^{2r-1} = \zeta$; but then (5) says

$$x - \zeta^2 x \equiv 0 (\text{mod } p),$$

and Lemma 2.4 implies that $p \mid x$, which contradicts our original assumption.

This completes the proof.

Remark 2.1. Under the assumption that the domain $\mathbb{Z}[\zeta_p]$ has unique factorization property can we prove the first case of Fermat's Last Theorem. But $\mathbb{Z}[\zeta_p]$ is UFD only for few primes. In 1971, Montgomery and Ushid independently obtained that ζ_p is a UFD only for prime $p = 3, 5, 7, 11, 13, 17, 19$. If we extend the restriction on the primality of n, there are still few integers such that $\mathbb{Z}[\zeta_n]$ is UFD. Actually, in 1975, Masley and Montgomery proved that there are precisely 29 values of $n > 1$, $n \not\equiv 2 (\text{mod } 4)$ for which $\mathbb{Z}[\zeta_n]$ is a UFD. These are

$$n = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

Remark 2.2. The *ABC conjecture* (also known as the Oesterlé-Masser conjecture) is a conjecture in number theory, first proposed by Joseph Oesterlé and David Masser in 1985. It is stated in terms of three positive integers, a, b and c that are relatively prime and satisfy $a + b = c$. If d denotes the product of the distinct prime factors of abc, the conjecture essentially states that d is usually not much smaller than c. In other words: if a and b are composed from large powers of primes, then c is usually not divisible by large powers of primes. For example, let $a = 2, b = 3^{10} \cdot 109 = 6436341, c = 23^5 = 6436343$, one can see $a + b = c$ and $\text{rad}(abc) = 2 \cdot 3 \cdot 23 \cdot 109 = 15042$, where $\text{rad}(n)$ denotes the product of the distinct prime factors of n. Then 15042 is not much smaller than 6436343.

The precise formulation of ABC conjecture states as follows. For every positive real number ε, there exist only finitely many triples (a, b, c) of coprime positive integers, with $a + b = c$, such that

$$c > \text{rad}(abc)^{1+\varepsilon}.$$

A number of famous conjectures and theorems in number theory would follow immediately from the abc conjecture or its versions. For example, the ABC conjecture implies Fermat's Last Theorem. Goldfeld (1996) described the abc conjecture as "the most important unsolved problem in Diophantine analysis". Currently ABC conjecture is still open, but Fermat's Last Theorem had been proved.

In August 2012 Shinichi Mochizuki claimed a proof of the abc conjecture. He released a series of four preprints developing a new theory called Inter-universal Teichmüller theory which is then applied to prove several famous conjectures in number theory, including the abc conjecture but also Szpiro's conjecture, the hyperbolic Vojta's conjecture. The papers are not accepted by the mathematical community as providing a proof of ABC. This is not only because of their impenetrability, but also because at least one specific point in the argument has been identified as an unfixable gap by some other experts. Though a small circle of mathematicians have vouched for the correctness of the proof, and have attempted to communicate their understanding via workshops on inter-universal Teichmüller theory, this has failed to convince the number theory community at large. In September 2018, Peter Scholze and Jakob Stix published a report detailing the (previously identified) gap in the proof, describing it as "so severe that in [their] opinion small modifications will not rescue the proof strategy".

(For details, see see https://en.wikipedia.org/wiki/Abc_conjecture)

Exercises

1. Describe Fermat's Last Theorem.

2. Express $\frac{1-\zeta_{23}^4}{1-\zeta_{23}^9}$ in the form $\zeta_{23}^r u$ according to Lemma 2.5, where $0 \le r \le 22$ and u is a real unit.

3. Prove Lemma 2.5.

4. Let n be a positive integer and $\mathrm{rad}(n)$ denote the product of the distinct prime factors of n. For odd prime integer p, let $a = 1, b = 2^{p(p-1)n} - 1, c = 2^{p(p-1)n}$. Show that $a + b = c$ and
$$\mathrm{rad}(abc) < \frac{2}{p}c.$$
In particular, $\mathrm{rad}(abc) < c$.

5. With the help of Fermat's Last Theorem, solve the following problems.

   (1) Let $f(x) = \frac{1803664}{1+1803664x} + \frac{2298565}{1+2298565x} - \frac{2301505}{1+2301505x}$. Prove that $f^{(16)}(0) \neq 0$.

   (2) What is the number of distinct positive integers n such that $n+3^2$ and n^2+3^3 are both perfect cubes?

   (3) Find the number of positive integers n such that there exists an integer $m \neq \frac{n}{2}$ such that $\frac{n^3-2m^3}{6m}$ is a perfect square.

   (4) Let n be a positive integer which makes $x = \frac{n}{3}(4n^2+6n+3)$ a triangular number. How many solutions are there for n?

3 Field of Fractions

In this section, we suppose that R is a (commutative) domain. Let R^* denote the set of non-zero elements of R. That is,
$$R^* = \{a \in R \mid a \neq 0\}. \tag{6}$$

We propose a relation " $\sim$ " in the Cartesian product $R \times R^* = \{(a, b) \mid a \in R, b \in R^*\}$ by defining
$$(a, b) \sim (c, d) \text{ if and only if } ad = bc. \tag{7}$$

One can easily check that $\sim$ defines an equivalence relation in $R \times R^*$. For simplicity, we write $\frac{a}{b}$ (or a/b) for the equivalence relation of (a, b) in $R \times R^*$, where $a \in R, b \in R^*$. Thus,
$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc. \tag{8}$$
For example, $\frac{ax}{bx} = \frac{a}{b}$ for any $x \in R^*$.

Denote
$$Q(R) = \left\{ \frac{a}{b} \mid a \in R, b \in R^* \right\}. \tag{9}$$

Now we define the operations in $Q(R)$ as follows. For $\frac{a}{b}, \frac{c}{d} \in Q(R)$, define
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{10}$$

We first check that the operation is well-defined. Suppose $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$. Then $ab' = a'b, cd' = c'd$ and we have
$$(ad+bc)b'd' = ab' \cdot d'd + bb' \cdot cd' = a'b \cdot d'd + bb' \cdot c'd = (a'd' + b'c')bd.$$

Hence $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. Similarly $acb'd' = a'c'bd$ implies that $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. This shows that the operations are independent of the representation of the elements of $Q(R)$.

Theorem 3.1. *The set $Q(R)$ together with the addition and multiplication given by (10) is a field. The element $\frac{0}{1}$ is the zero element and $\frac{1}{1}$ is the identity.*

The proof is straightforward. One only need to verify them term by term. For example, if $\frac{a}{b} \neq 0$ in $Q(R)$, then $a \neq 0$. Hence $\frac{b}{a} \in Q(R)$. That is, $\frac{a}{b}$ is a unit with

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

The field $Q(R)$ is called the **field of fractions** (分式域) or **quotient filed**(商域) of R.

Example 3.1. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. That is, $Q(\mathbb{Z}) = \mathbb{Q}$.

Example 3.2. If R is itself a field, then $Q(R) = R$.

Theorem 3.2. 1. *The natural map*

$$\begin{aligned} \tau : R &\to Q(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

is a monomorphism of rings. In particular, a domain can be embedded in a field.

2. *If we identify R with its image in $Q(R)$, then R is a subring of $Q(R)$ and the field of fractions is the smallest field containing R.*

The proof is clear.

> The field of fractions of a domain may be regarded as the smallest field containing it.

We may embed each domain in its field of fractions to achieve a refinement of the division algorithm.

Proposition 3.1. *Let R be a domain and $f(x), g(x) \in R[x]$. If $g(x) \neq 0$, we have $a \in R$ and $q(x), r(x) \in R[x]$ such that*

$$af(x) = g(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Exercises

1. Let R be a domain and F a field. Suppose that there is a ring homomorphism σ from R to F. Show that there is a unique ring homomorphism σ' from $Q(R)$ to F such that the restriction of σ' to R is σ, i.e. $\sigma'(a) = \sigma(a)$ for all $a \in R$. The homomorphism σ' is called an *extension* of σ.

2. Describe the field of fractions of $\mathbb{Z}[\alpha]$, where α is a zero of $x^2 - 4x + 2$.

3. Let α be an algebraic number. Show that $\mathbb{Q}[\alpha]$ is the field of fractions of $\mathbb{Z}[\alpha]$.