The Ramanujan-Nagell Theorem: Understanding the Proof

By Spencer De Chenne

1 Introduction

The Ramanujan-Nagell Theorem, first proposed as a conjecture by Srinivasa Ramanujan in 1943 and later proven by Trygve Nagell in 1948, largely owes its proof to Algebraic Number Theory (ANT). As the reader might have taken from the name, ANT expands and often relies on results from ordinary Number Theory; however, as ANT should be read as the theory of *Algebraic Numbers*, it is natural to think of ANT as an extension of Abstract Algebra, and as such the reader should be familiar with many results from Abstract Algebra, and especially confident with their basic understanding of Fields.

More specifically, while Number Theory focuses largely on the study of the integers, $\mathbb{N}$, ANT focuses on the rational numbers, $\mathbb{Q}$, and extensions of $\mathbb{Q}$. In this manner, we shall begin by showing some preliminary results and definitions.

2 Algebraic Number Theory Essentials

Theorem 1: The set $\overline{\mathbb{Q}}$ of all algebraic numbers over $\mathbb{Q}$ is a subfield of $\mathbb{C}$.

Proof. We will use the result from Abstract Algebra that for $\alpha \in E$, for a fields F and $E = F(\alpha)$, α is algebraic if and only if $[E : F]$ is finite. Now suppose that α and β are algebraic over $\mathbb{Q}$. Then

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Now, since β is algebraic over $\mathbb{Q}$, it must certainly be algebraic over $\mathbb{Q}(\alpha)$ and the extension must be finite, and since α is algebraic over $\mathbb{Q}$ this extension must also be finite. Therefore, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is finite and $\mathbb{Q}(\alpha, \beta)$ must be a finite extension over $\mathbb{Q}$. Furthermore, $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β (for $\beta \neq 0$) must belong to $\mathbb{Q}(\alpha, \beta)$. Thus, in this way, adjoining algebraic elements will always result in finite extensions, and $\overline{\mathbb{Q}}$ must be a subfield of $\mathbb{C}$. □

While $\overline{\mathbb{Q}}$ may not be very interesting in its entirety (due perhaps to the fact that $[\overline{\mathbb{Q}} : \mathbb{Q}]$ is not finite), we are very interested in *number fields*, which are subfields K of $\mathbb{C}$ such that $[K : \mathbb{Q}]$ is finite. This implies that every element of K is algebraic, and hence K is a subfield of $\overline{\mathbb{Q}}$.

Just as Abstract Algebra generalizes many concepts the reader learned in high school, ANT generalizes many results and concepts from ordinary Number Theory. One such interesting and important concept is a generalization of the integers, known as *algebraic integers*. Similar to the definition of algebraic numbers, an algebraic integer is a complex number α such that α is the root of a monic polynomial $p(x) \in \mathbb{Z}[x]$; in other words,

$$p(\alpha) = \sum_{i=0}^{n} k_i \alpha^i = 0$$

for $k_i \in \mathbb{Z}$, $k_n = 1$. It is easy to observe that not every element of $\mathbb{Q}$ is an algebraic integer. Take, as an example, $\phi = 22/7$, which is a root of the polynomial $q(x) = 7x - 22$, which is not monic, and $s(x) = x - 22/7 \notin \mathbb{Z}[x]$. Further studies shall be conducted in finite extensions of $\mathbb{Q}$, and often we are concerned with the algebraic integers of such extension fields. For this reason, we shall show some preliminary results about the algebraic integers, denoted $\mathbb{A}$.

Theorem 2: The algebraic integers form a subring of the field of algebraic numbers.

Proof. We must show that for $\alpha, \beta \in \mathbb{A}$, $\alpha + \beta \in \mathbb{A}$ and $\alpha\beta \in \mathbb{A}$. Suffice it to say that for $\phi \in \mathbb{C}$, ϕ is algebraic if and only if the additive group generated by all powers $1, \phi, \phi^2, ...$ is finitely generated. From this we can claim that the powers of $\alpha + \beta$ and $\alpha\beta$ lie in a finitely generated subgroup of $\mathbb{C}$, and so $\alpha + \beta$ and $\alpha\beta$ are algebraic. Hence, $\mathbb{A}$ forms a subring of $\overline{\mathbb{Q}}$. □

Theorem 3: An algebraic number α is an algebraic integer if and only if its minimum polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Proof. Let $p(x)$ be the minimum polynomial of α over $\mathbb{Q}$, and recall that this is both monic and irreducible in $\mathbb{Q}[x]$. If $p(x) \in \mathbb{Z}[x]$, then α if an algebraic integer. Conversely, if α is algebraic, then $q(\alpha) = 0$ for some $q(x) \in \mathbb{Z}[x]$, and $p|q$. It follows that $p \in \mathbb{Z}[x]$ because some rational multiple $\gamma p \in \mathbb{Z}[x]$ and divides q, and the monicity of q implies $\gamma = 1$. □

Similar to $\overline{\mathbb{Q}}$, we are rarely interested in the entirety of $\mathbb{A}$; however, for finite extensions of $\mathbb{Q}$, we are often interested in the algebraic integers contained in the field. For an extension field K over $\mathbb{Q}$, we define the *ring of integers* of K as

$$\mathfrak{O}_K = K \cap \mathbb{A}.$$

Since both $\mathbb{A}$ and K are subrings of $\mathbb{C}$, then it follows that $\mathfrak{O}_K$ is a subring of K. Furthermore, because $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ and $\mathbb{Z} \subseteq \mathbb{A}$, then $\mathbb{Z} \subseteq \mathfrak{O}_K$. With the concept of algebraic integers, we can redefine modular arithmetic in a natural way. We say that for $\alpha, \beta, \gamma \in \mathfrak{O}_K$, if

$$\alpha \equiv \beta \pmod{\gamma},$$

then $\alpha = \gamma\phi + \beta$ for some $\phi \in \mathfrak{O}_K$. To demonstrate this concept, we shall use an example that will illuminate methods of verification as well as serve us in a future proof.

Example: For $a, b \in \mathbb{Q}(\sqrt{-7})$, consider

$$a = \frac{1 + \sqrt{-7}}{2} \qquad \text{and} \qquad b = \frac{1 - \sqrt{-7}}{2}.$$

It is simple to verify that a^2 and b^2 are both algebraic integers (as well as conjugates) because they both satisfy the polynomial $p(x) = x^2 + 3x + 4$. We claim that

$$a^2 \equiv 1 \pmod{b^2}.$$

To verify this, consider the quotient

$$\frac{a^2 - 1}{b^2} = \frac{1 - \sqrt{-7}}{2}.$$

We leave it to the reader to verify that the quotient is a root of $x^2 - x + 2$, a monic polynomial with coefficients in $\mathbb{Z}$.

Now that we have defined what modular arithmetic with algebraic integers is, we can state the following theorem that will be useful in understanding the Ramanujan-Nagell Theorem. Keep in mind that a *squarefree rational integer* is an element $a \in \mathbb{Z}$ such that the prime factorization of a has no squared factors.

Theorem 4: Let d be a squarefree rational integer. Then the integers of $\mathbb{Q}(\sqrt{d})$ are:

1. $\mathbb{Z}\left[\sqrt{d}\right]$ if $d \not\equiv 1 \pmod 4$,
2. $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$ if $d \equiv 1 \pmod 4$

Proof. Every element $\alpha \in \mathbb{Q}(\sqrt{d})$ is of the form $\alpha = r + s\sqrt{d}$, for $r, s \in \mathbb{Q}$. Hence, we may write

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

where $a, b, c \in \mathbb{Z}, c > 0$, and no primes divide every a, b, and c. Now α is an integer if and only if the coefficients of the minimum polynomial

$$\left(x - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(x - \left(\frac{a - b\sqrt{d}}{c}\right)\right)$$

are integers. Thus,

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}, \tag{1}$$

$$\frac{2a}{c} \in \mathbb{Z}. \tag{2}$$

If c and a have a common prime factor p then (1) implies that p divides b (since d is squarefree) which contradicts our previous assumption. Hence, from (2) we have $c = 1$ or 2. If $c = 1$, then α is an integer of $\mathbb{Q}(\sqrt{d})$ in any case, so we may concentrate on the case $c = 2$. Now a and b must both be odd, and $(a^2 - b^2 d)/4 \in \mathbb{Z}$. Hence,

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

Now, and odd number $2k + 1$ has square $2k^2 + 4k + 1 \equiv 1 \pmod 4$, hence $a^2 \equiv 1 \equiv b^2 \pmod 4$, and this implies $d \equiv 1 \pmod 4$. Conversely, if $d \equiv 1 \pmod 4$ then for odd a, b we have α an integer because (1) and (2) hold.

To sum up: if $d \not\equiv 1 \pmod 4$, then $c = 1$ and so (1) holds; whereas if $d \equiv 1 \pmod 4$ we can also have $c = 2$ and a and b odd, whence easily (2) holds. □

The reader may be interested to know that such fields are called *quadratic fields* if they are a degree 2 extension over $\mathbb{Q}$. In the case where d is positive, such fields are known as *real* fields,

whereas if d is negative the fields are known as *imaginary* fields. Currently, as the reader may have guessed, we are interested in the latter. Consider another example of the imaginary quadratic field $\mathbb{Q}(\sqrt{-7})$:

Example: $-7 \equiv 1 \pmod 4$, which implies that the integers of $\mathbb{Q}(\sqrt{-7})$ are $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\right]$.

In order to prove some upcoming theorems, the reader should be familiar with some results from field theory. The following theorem should seem both familiar and new.

Theorem 5: Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms $\sigma_i : K \mapsto \mathbb{C}$ $(i = 1, ..., n)$ which fix $\mathbb{Q}$ element-wise. The elements $\sigma_i(\alpha) = \alpha_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of α over $\mathbb{Q}$.

Proof. It is an important and non-trivial result that an irreducible polynomial over a subfield K of $\mathbb{C}$ has no repeated roots in $\mathbb{C}$; however, this result will not be proved here. Let $\alpha_1, ..., \alpha_n$ be the n distinct roots of the minimum polynomial $p(x)$ of α guaranteed by this result. Then each α_i also has minimum polynomial $p(x)$, and so there is a unique field isomorphism $\sigma_i : \mathbb{Q}(\alpha) \mapsto \mathbb{Q}(\alpha_i)$ such that $\sigma_i(\alpha) = \alpha_i$. In fact, if $\beta \in \mathbb{Q}(\alpha)$ then $\beta = r(\alpha)$ for a unique $r \in \mathbb{Q}[x]$ with $\deg(r) < n$; and we must have

$$\sigma_i(\beta) = r(\alpha_i).$$

Conversely, if $\sigma : K \mapsto \mathbb{C}$ is a monomorphism then σ is the identity on $\mathbb{Q}$. Then we have

$$0 = \sigma(p(\alpha)) = p(\sigma(\alpha))$$

so that $\sigma(\alpha)$ is one of the α_i, hence σ is one of the σ_i. □

Example: Consider the field $\mathbb{Q}(\sqrt{-7})$. Because this is a degree 2 extension over $\mathbb{Q}$ and both roots of the minimal polynomial of $\sqrt{-7}$ are contained in $\mathbb{Q}(\sqrt{-7})$, there must be exactly two automorphisms that fix $\mathbb{Q}$ element-wise. The automorphisms are then:

$$\sigma_1(a + b\sqrt{-7}) = a + b\sqrt{-7}$$
$$\sigma_2(a + b\sqrt{-7}) = a - b\sqrt{-7}$$

This specific result, resembling previous studies in abstract algebra, aids us in the following definition:

Definition: Let $K = \mathbb{Q}(\alpha)$ be a degree n extension. The *norm* of $\beta \in K$ is

$$N_K(\beta) = \prod_{i=1}^{n} \sigma_i(\beta),$$

where the σ_i are the monomorphisms previously defined.

Example: Consider again $K = \mathbb{Q}(\sqrt{-7})$, and let $\alpha = a + b\sqrt{-7} \in K$. Then

$$N_K(\alpha) = (a + b\sqrt{-7})(a - b\sqrt{-7}) = a^2 - 7b^2.$$

At this point, we leave it to the reader to remind themselves of the definitions of primes, units and Noetherian rings, as these are important concepts in the following section. The reader should be aware that for an integral domain D, factorization into irreducibles is possible if D is Noetherian. Furthermore, for a number field K, $\mathfrak{O}_K$ is Noetherian (the proof will not be given here, as it requires more theory of free groups than is expected of the reader). From this, it is a direct corollary to state that factorization into irreducibles is possible in $\mathfrak{O}_K$. The following theorem discusses units in specific fields:

Theorem 6: The group of units U of the integers in $\mathbb{Q}(\sqrt{d})$ where d is negative and squarefree is as follows:

1. For $d = -1$, $U = \{\pm 1, \pm i\}$
2. For $d = -3$, $U = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}$ where $\omega = e^{2\pi i/3}$
3. For all other $d < 0$, $U = \{\pm 1\}$

The proof of this theorem is too broad to be added to this paper. For clarification, the reader can refer to Stewart and Tall's *Algebraic Number Theory*. As one might have gathered, our primary interest is in the field $\mathbb{Q}(\sqrt{-7})$. The implication of this theorem is that we can now confidently state that the group of units of this field is $\{\pm 1\}$.

The following theorem ties together many previous ideas and is perhaps the most powerful in our proof of the Ramanujan-Nagell theorem, as it addresses factorization in number fields.

Theorem 7: Let $\mathfrak{O}_K$ be the ring of integers of a number field K, and let $x, y \in \mathfrak{O}_K$. Then

1. x is a unit if and only if $N(x) = \pm 1$,
2. If x and y are associates, then $N(x) = \pm N(y)$,
3. If $N(x)$ is a rational prime, then x is irreducible in $\mathfrak{O}_K$.

Proof. 1.) if $xu = 1$, then $N(x)N(u) = 1$. Since $N(x), N(u) \in \mathbb{Z}$ (see Stewart and Tall's *Algebraic Number Theory*), we have $N(x) = \pm 1$, then

$$\sigma_1(x)\sigma_2(x)...\sigma_n(x) = \pm 1$$

which is the definition of the norm of x. One factor, without loss of generality $\sigma_1(x)$, is equal to x (from the identity mapping); all other $\sigma_i(x)$ are integers. Put

$$u = \pm\sigma_2(x)...\sigma_n(x).$$

Then $xu = 1$, so $u = x^{-1} \in K$. Hence $u \in K \cap \mathbb{A} = \mathfrak{O}$, and x is a unit.

2.) If x, y are associates, then $x = uy$ for a unit u, so $N(x) = N(uy) = N(u)N(y) = \pm N(y)$ by 1.).

3.) Let $x = yz$. Then $N(y)N(z) = N(yz) = N(x) = p$, a rational prime; so one of $N(y)$ and $N(z)$ is $\pm p$ and the other is ± 1. By 1.), one of y and z is a unit, so x is irreducible.

□

The following theorem will not be proven here due to both the proof's length and complexity; however, we are interested in only one of the results from the theorem, which will validate many of the conclusions drawn in the Ramanujan-Nagell Theorem.

Theorem 8: The ring of integers $\mathfrak{O}$ of $\mathbb{Q}(\sqrt{-7})$ is Euclidian for $d = -1, -2, -3, -7, -11$, with Euclidian valuation

$$\phi(\alpha) = |N(\alpha)|.$$

Proof. See Stewart and Tall's *Algebraic Number Theory.* □

At this point, the reader should review examples previously stated in the text, as every single one was created in order to ease some of the understanding of the following section. As one could gather, the following section focuses on applications of the learned material in the field $\mathbb{Q}(\sqrt{-7})$.

3 The Ramanujan-Nagell Theorem

Questions in Algebraic Number Theory often seem at first glance to be questions in ordinary Number Theory. The Ramanujan-Nagell Theorem is such a theorem, whose conclusion is about the integer solutions to an equation. However, we shall see that the proof utilizes field extensions and properties of unique factorization in order to state that the presented solutions are the *only* solutions to the equation.

Theorem (Ramanujan-Nagell): The only solutions to the equation

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

for $x, n \in \mathbb{Z}$ are

$\pm x = 1$	3	5	11	81
$n = 3$	4	5	7	15.

Proof. We will work in $\mathbb{Q}(\sqrt{-7})$, whose ring of integers has unique factorization. Clearly, x must be odd, and we see that for (x, n) which satisfies the equation, $(-x, n)$ too must satisfy the equation, and so we will assume x to be positive.

First, we assume that n is even, in which case we have the factorization

$$\begin{aligned} 7 &= 2^n - x^2 \\ &= (2^{n/2} - x)(2^{n/2} + x). \end{aligned}$$

Clearly, both $2^{n/2} - x$ and $2^{n/2} + x$ must be integers. Because x is assumed positive and $n > 0$, then $2^{n/2} + x > 2^{n/2} - x$, and we find that

$$\begin{aligned} 7 &= 2^{n/2} + x \\ 1 &= 2^{n/2} - x, \end{aligned}$$

from which we observe

$$8 = 2^{1+n/2}.$$

Thus, $n = 4$, and we find that $x = 3$.

Now let n be odd, and assume $n > 3$. We can see that

$$2 = \left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right)$$

is a factorization into primes. Obviously, x must be odd, so let $x = 2k+1$, implying that $x^2+7 = 4k^2+4k+8$ is divisible by 4. We can substitute $m = n-2$ and rewrite the original equation to be solved as

$$\frac{x^2+7}{4} = 2^m,$$

so that

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^m\left(\frac{1-\sqrt{-7}}{2}\right)^m,$$

where the right-hand side is a prime factorization. Neither $\frac{1+\sqrt{-7}}{2}$ nor $\frac{1-\sqrt{-7}}{2}$ is a common factor of the left-hand side, because such a factor would divide their difference, $\sqrt{-7}$, which is seen to be impossible by taking their norms. Comparing the two factorizations, since the only units of $\mathbb{Q}(\sqrt{-7})$ are ± 1 (which we showed previously), we must have

$$\frac{x\pm\sqrt{-7}}{2} = \pm\left(\frac{1\pm\sqrt{-7}}{2}\right)^m.$$

From this, we can see that

$$\begin{aligned}
\frac{x+\sqrt{-7}}{2} &= \left(\frac{1+\sqrt{-7}}{2}\right)^m,\\
\frac{x-\sqrt{-7}}{2} &= \left(\frac{1-\sqrt{-7}}{2}\right)^m,\\
\frac{x+\sqrt{-7}}{2} &= \left(\frac{1-\sqrt{-7}}{2}\right)^m,\\
\frac{x-\sqrt{-7}}{2} &= \left(\frac{1+\sqrt{-7}}{2}\right)^m.
\end{aligned}$$

By taking differences of these equations, we derive that

$$\pm\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m.$$

We claim that

$$+\sqrt{-7} \neq \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m.$$

For conciseness, we let $a = \left(\frac{1+\sqrt{-7}}{2}\right)$ and $b = \left(\frac{1-\sqrt{-7}}{2}\right)$, observing that $a-b = \sqrt{-7}$. Therefore,

$$a - b = a^m - b^m.$$

Then,

$$a^2 \equiv (1-b)^2 \equiv 0 \pmod{b^2}$$

since $ab = 2$, and so

$$a^m \equiv a(a^2)^{(m-1)/2} \equiv a \pmod{b^2}$$

whence

$$a \equiv a - b \pmod{b^2},$$

which is a contradiction.

Hence, the sign must be negative. Observe that we can rewrite the original statement as

$$\begin{aligned} -2^m\sqrt{-7} &= (1+\sqrt{-7})^m - (1-\sqrt{-7})^m, \\ &= \sum_{i=0}^{m} \binom{m}{i} (\sqrt{-7})^i - \sum_{i=0}^{m} \binom{m}{i} (-\sqrt{-7})^i. \end{aligned}$$

Now consider each i^{th} iteration of the sum. Suppose i is odd. Then the right-hand side becomes

$$\begin{aligned} \binom{m}{i}(\sqrt{-7})^i - \binom{m}{i}(-\sqrt{-7})^i &= \binom{m}{i}(\sqrt{-7} + \sqrt{-7}) \\ &= 2\binom{m}{i}(\sqrt{-7})^{i+1}. \end{aligned}$$

Now suppose i is even. Then the right-hand side becomes

$$\begin{aligned} \binom{m}{i}(\sqrt{-7})^i - \binom{m}{i}(-\sqrt{-7})^i &= \binom{m}{i}(\sqrt{-7} - \sqrt{-7}) \\ &= 0. \end{aligned}$$

Therefore,

$$-2^{m-1} = \binom{m}{1} - \binom{m}{3}7 + \binom{m}{5}7^2 - ... \pm \binom{m}{m}7^{\frac{m-1}{2}},$$

and we observe that $-2^{m-1} \equiv m \pmod 7$. Now, $2^6 \equiv 1 \pmod 7$, and it easily follows that the only solutions are then $m \equiv 3$, 5, or $13 \pmod{42}$.

We prove that only $m = 3$, 5, and 13 can occur, and to prove uniqueness it suffices to show that we cannot have two solutions of the original equation which are congruent modulo 42. So let m, m_1 be two such solutions, and 7^l be the largest power of 7 dividing $m - m_1$. Then

$$a^{m_1} = a^m a^{m_1 - m} = a^m (1/2)^{m_1 - m}(1+\sqrt{-7})^{m_1 - m}.$$

Now,

$$\left(\frac{1}{2}\right)^{m_1-m} = \left[\left(\frac{1}{2}\right)^6\right]^{\frac{m_1-m}{6}} \equiv 1 \pmod{7^{l+1}},$$

and

$$(1+\sqrt{-7})^{m_1-m} \equiv 1 + (m_1 - m)\sqrt{-7} \pmod{7^{l+1}}$$

(first raise to powers 7, 7^2, ..., 7^l, then $(m - m_1)/7$. Since

$$a^m \equiv \frac{1 + m\sqrt{-7}}{2^m} \pmod 7,$$

substituting gives

$$a^{m_1} \equiv a^m + \frac{m_1 - m}{2}\sqrt{-7} \pmod{7^{l+1}},$$

and

$$b^{m_1} \equiv b^m - \frac{m_1 - m}{2}\sqrt{-7} \pmod{7^{l+1}}.$$

But $a^m - b^m = a^{m_1} - b^{m_1}$, so $(m_1 - m)\sqrt{-7} \equiv 0 \pmod{7^{l+1}}$, but since m_1 and m are rational integers,

$$m_1 \equiv m \pmod{7^{l+1}},$$

contradicting the definition of l. Thus, $m = 3$, 5, or 13, which implies that $n = 5$, 7, and 15, and solutions for x can easily be found.

□

The interesting aspects of this proof are the points of confluence between abstract algebra and number theory. While the hypothesis stated the uniqueness of integer solutions, the elements that were considered belonged to an imaginary quadratic field. In this manner, many questions seemingly posed in number theory have proofs in ANT, such as Wile's famous proof of Fermat's Last Theorem in 1994. Ideas extending previous concepts are extremely useful to the progress of mathematics, and should be embraced and studied extensively as Algebraic Number Theory has been.

4 Bibliography

[1]Stewart I.N. and D.O. Tall. *Algebraic Number Theory*. Chapman and Hall: London. 1987.

[2]Mollim, Richard A. *Algebraic Number Theory*. Chapman and Hall: London. 1999.

[3]Pollard, Harry. *The Theory of Algebraic Numbers*. The Mathematical Association of America: Baltimore. 1950.

[4]Ono, Takashi. *An Introduction to Algebraic Number Theory*. Plenum Press: London. 1990.

5 Copyright