Quadratic Fields and Transcendental Numbers

Mohammad Zaki, MN State Univ, Mankato

We define an algebraic number α as a root of an algebraic equation, $a_0 * x^n + a_1 * x^{n-1} + \cdots + a_{n-1} * x + a_n = 0$ where $a_o, a_1, \cdots, a_n$ are rational integers, not all zero. We say α is an algebraic integer if $a_0 = 0$. If an algebraic number α satisfies an algebraic equation of degree n with rational coefficients, and none of lower degree, then we say α is of degree n.

If α is an algebraic number, then we define an algebraic field as the aggregate of all numbers $R(\alpha) = \frac{P(\alpha)}{Q(\alpha)}$, where P,Q are polynomials with rational coefficients, and $Q(\alpha) \neq 0$. We denote this field by K(α). It is easy to verify that the sum and product of any two members of K(θ) belong to K(θ). Also if $\alpha,\ \beta$ belong to K(θ) and $\beta \neq 0$ then $\frac{\alpha}{\beta}$ belongs to K(θ).

If an algebraic number ε is of degree 1, then ε is a rational number, and it is plain that for any rational ε $K(\varepsilon)$ is the aggregate of rational numbers. We denote this field by $K(1)$. It is a part of every algebraic field.

If the degree of ε is 2, then ε is said to be quadratic, and K(ε) is called a quadratic field. Since the degree of ε is 2 ε satisfies a quadratic equation, $a_0 * x^2 + a_1 * x + a_2 = 0$. so, $\varepsilon = a + b * \sqrt{m}/c$ for some integers a, b, c, m where m doesn't have a squared factor. It is easily verified that $K(\varepsilon)$ is the same as $K(\sqrt{m})$ for some square-free rational integer m, positive or negative, apart from 1.

Here we concentrate on quadratic fields. We will try to find the quadratic fields where the fundamental theorem of arithmetic holds. But before we get there we need to develop the notion of primes, and the Euclidean Property that will be described in a moment.

If $\varepsilon \in K(\sqrt{m})$ then

$$\begin{aligned} \varepsilon = \frac{P(\sqrt{m})}{Q(\sqrt{m})} &= s + t * \sqrt{m}/u + v\sqrt{m} \\ &= \frac{<(s+t*\sqrt{m})*(u-v*sqrtm)>}{<(u^2-v^2*m)>} \\ &= \frac{<a+b*\sqrt{m}>}{<c>} \end{aligned}$$

for some rational integers s, t, u, v, a, b, c. So we have if $\varepsilon \in K(\sqrt{m})$ then $(c * \varepsilon - a)^2 - mb^2 = 0$. Thus ε is a root of a quadratic equation. Hence every $\varepsilon \in K(\sqrt{m})$ is either a rational or a quadratic.

Now we want to characterize the integers of $K(\sqrt{m})$. Recall that $\varepsilon \in K(\sqrt{m})$) is an (algebraic) integer if it satisfies an equation $x^j + a_1 * x^(j-1) + \cdots + a_j = 0$ for some j. We can show that if ε is an integer then there is a unique equation with $j = 1$ satisfied by ε. To do this, we define a primitive polynomial as an integral polynomial, $f(x) = a_0 * x^n + a_1 x^(n-1) + \cdots + a_n$ where $a_0 > 0$ and $\gcd(a_0, a_1, \cdots, a_n) = 1$. We call $f(x) = 0$ a primitive equation.

Let's state a theorem that implies the assertion about j being 2.

Theorem 1. *Let ε be an algebraic number of degree n, and let $f(x) = 0$ be a primitive equation of degree n satisfied by ε. If $g(x) = 0$ is any primitive equation satisfied by ε then $g(x) = f(x) \cdot h(x)$ for some primitive polynomial $h(x)$ and for all x.*

Corollary. *An algebraic number ε of degree n satisfies a unique primitive equation of degree n, and if ε is an integer then the coefficient of x^n in this equation is* 1.

From this Corollary we see that our assertion about j being 2 is right. So we can say that if $\varepsilon \in K(\sqrt{m})$ is an integer then ε satisfies a unique quadratic equation with leading coefficient 1. As a matter of fact, we can do better in characterizing the integers.

Theorem. *The integers of $K(\sqrt{m})$ are as follows. The integers of $K(\sqrt{m})$ are the numbers $a + b \cdot \sqrt{m}$ when $m = 2(mod 4)$ or $m = 3(mod 4)$, and the numbers $a + b \cdot \omega$ where $\omega = \frac{1}{2} \cdot (\sqrt{m} - 1)$ when $m = 1(mod 4)$. a, b are, in either case, rational integers. (We won't prove this, but it's not too hard.)*

For example, consider $K(i)$ and $K(\sqrt{-3})$. The integers of $K(i)$ are of the form $a + b \cdot i$, a and b being rational integers since $-1 = 3(mod 4)$. On the other hand, since $-3 = 1(mod 4)$, the integers of $K(\sqrt{-3})$ are the numbers $a + \frac{1}{2} \cdot b \cdot (\sqrt{-3} - 1)$, a and b being rational integers.

Now we are ready to develop the notion of primes in quadratic fields. We need some definitions at this point.

Let α, β be integers. We say α is divisible by β if there exists another integer γ such that $\alpha = \beta \cdot \gamma$. If α is divisible by β then we also say that β divides α, and write $\beta | \alpha$. We define a unit ϵ as a divisor of 1

(and therefore of every integer of the field). For every integer ε, $\epsilon \cdot \varepsilon$ is called an *associate* of ε. We define a *prime* as an integer which is only divisible by units and by its own associates. We call $\bar{\epsilon} = r - s \cdot \sqrt{m}$ the conjugate of $\epsilon = r + s \cdot \sqrt{m}$ where r, s are rationals. The norm $N\epsilon$ of ϵ is defined by

$$N\epsilon = \epsilon \cdot \bar{\epsilon} = r^2 - m \cdot s^2$$

It is clear that the norm of an integer of $K(\sqrt{m})$ is a rational integer.

If m¿0 we call $K(\sqrt{m})$ a *real* field, and if mj0 then we call $K(\sqrt{m})$ a *complex* field. Norms are positive in complex fields, but not necessarily in real fields. We can prove the following two results.

Theorem 2. *If ϵ_1 and ϵ_2 are units, then $\epsilon_1 \cdot \epsilon_2$ and ϵ_1/ϵ_2 are units.*

Theorem 3. *The norm of a unit is $+1$ or -1, and every number whose norm is 1 or -1 is a unit.*

Theorem 4. *An integer whose norm is a rational prime is a prime.*

Theorem 5. *An integer, not 0 or a unit, is divisible by a prime.*

proof(5): Let γ be an integer. If γ is not a prime, then there are integers α_1 and β_1 such that $\gamma = \alpha_1 \cdot \beta_1$, $|N\alpha_1| > 1$, $|N\beta_1| > 1$, and $|N\gamma| = |N\alpha_1| \cdot |N\beta_1|$. If α_1 is not a prime, then there are integers α_2 and β_2 such that $\alpha_1 = \alpha_2 \cdot \beta_2$, $|N\alpha_2| > 1$, $|N\beta_2| > 1$, and $|N\alpha_1| = |N\alpha_2| \cdot |N\beta_2|$. Also, $1 < |N\alpha_2| < |N\alpha 1|$. If we continue this process, since $|N\gamma|, |N\alpha 1|, |N\alpha_2| \cdots$ is a decreasing sequence of positive rational integers, we will come to a prime α_n because $|N\alpha| = 0$ if and only if $\alpha = 0$. But this α_n divides γ. Hence, our claim is true.

Theorem 6. *Any integer, not 0 or a unit, is a product of primes. (This can be derived using theorem 5.)*

We say that the algebraic integers in $K(\sqrt{m})$ are a *Euclidean ring* if, given any two integers γ, γ_1, of which $\gamma_1 \neq 0$, there exist integers γ_2 and k such that $\gamma = k \cdot \gamma_1 + \gamma_2$ with $|N\gamma_2| < |N\gamma_1|$. If this holds in $K(\sqrt{m})$, then we say there is a *Euclidean algorithm* in $K(\sqrt{m})$, or we simply say that $K(\sqrt{m})$ is Euclidean. We know that the Euclidean property holds in the rational integers, and we can prove that $K(i)$, and $K(\sqrt{-3})$ are Euclidean.

Theorem 7. *The fundamental theorem of Unique Factorization, which states that any integer, not 0 or 1 can be expressed as a product of primes uniquely, apart from the order in which the primes are placed in the expression, the presence of units, and ambiguities between associated primes, is true in any Euclidean quadratic field.*

To prove this, we shall first obtain in $K(\sqrt{m})$ in an analogue of Euclid's algorithm, and define the notion of the greatest common divisor of two integers.

Assume, $K(\sqrt{m})$ is Euclidean. If γ, γ_1 are given integers and $\gamma_1 \neq 0$, then we get $\gamma = k \cdot \gamma_1 + \gamma_2$ with $|N\gamma_2| < |N\gamma_1|$ for some algebraic integers k and γ_2. If $\gamma_2 \neq 0$, then $\gamma_1 = k_1 \cdot \gamma_2 + \gamma_3$ with $|N\gamma_3| < |N\gamma_2|$, and so on. Thus, as $|N\gamma_1|, |N\gamma_2|, \cdots$ is a decreasing sequence of nonnegative rational integers, this process must come to an end. So, there must be an n such that $|N\gamma_{n+1}| = 0$, $\gamma_{n+1} = 0$. The last part of the algorithm is then $\gamma_{n-2} = k_{n-2} \cdot \gamma_{n-1} + \gamma_n$ and $\gamma_{n-1} = k_{n-1} \cdot \gamma_n$.

It follows that γ_n is a common divisor of γ and γ_1. To see this, note that γ_n divides γ_{n-1} which together with the equation $\gamma_{n-2} = k_{n-2} \cdot \gamma_{n-1} + \gamma_n$, implies that γ_n divides γ_{n-2}. Similarly γ_n divides γ_{n-3} and so on.

If α is a common divisor of γ, β, and every common divisor of γ, β divides α, then α is called the greatest common divisor of γ, β. We denote by (γ, β) the greatest common divisor of γ, β. The common divisor of ζ, η found by the Euclidean algorithm is the greatest.

The greatest common divisor is not unique, since any associate of the greatest common divisor is also a greatest common divisor. If ζ and η are both greatest common divisors, then ζ and η are associates. So we may say that the greatest common divisor is unique except for ambiguity between associates.

Theorem 8. *If $(\gamma, \gamma_1) = 1$ and $\gamma_1 | \beta \cdot \gamma$, then $\gamma_1 | \beta$.*

proof: Suppose $\gamma \neq 0$. Then Euclid's algorithm gives

$$\begin{array}{ccc} \gamma & = & k \cdot \gamma_1 + \gamma_2 \\ \gamma 1 & = & k_1 \cdot \gamma_2 + \gamma_3 \\ \cdots & & \\ \gamma_{n-2} & = & k_{n-2} \cdot \gamma_{n-1} + \gamma_n \\ \gamma_{n-1} & = & k_{n-1} \cdot \gamma_n \end{array}$$

If we multiply each line of this algorithm by β, we get $(\gamma \cdot \beta, \gamma_1 \cdot beta) = \beta \cdot \gamma_n$, but γ_n is a unit, and so $(\gamma \cdot \beta, \gamma_1 \cdot beta) = \beta$. By the hypothesis $\gamma_1 | \beta \cdot \gamma$ and hence γ_1 is a common divisor of $\gamma_1 \cdot \beta$ and $\gamma \cdot \beta$. Therefore, $\gamma_1 | \beta$ by the definition of the greatest common divisor.

Corollary. *If θ is a prime and $\theta | \beta \cdot \gamma$, then either $\theta | \beta$ or $\theta | \gamma$.*

It is obvious that if θ is a prime and $\theta | \beta \cdot \gamma \cdot \alpha \cdots$, then either $\theta | \beta$ or $\theta | \gamma$ or $\theta | \alpha$ and so on. The fundamental theorem follows from this Corollary.

Definition: A *simple* field is a field in which the fundamental theorem of Unique Factorization is true.

As we may guess now, the arithmetic of simple fields follows the lines of rational arithmetic. It is very difficult to determine all the simple fields. Siegel, Heilbronn, and other have proven that the number of simple complex quadratic fields is finite. Gauss essentially conjectured this.

Since in any Euclidean quadratic field, the fundamental theorem is true, every Euclidean quadratic field is simple. In what follows are some results that determines all the Euclidean quadratic fields. This is done by using the following equivalent statement to the Euclidean property. *Given any δ (integral or not) of $K(\sqrt{m}$, there exists an integer k such that $|N(\delta - k)| < 1$.*

Proof of equivalence: Assume $\delta = r + s \cdot \sqrt{m}$, where r and s are rationals. If $m \neq 1(mod 4)$ then we can write $k = x + y \cdot \sqrt{m}$ for x, y rational integers. So, $|(r-x)^2 - m \cdot (s-y)^2| = |N(\delta - k)| < 1$. On the other hand, if m=1 (mod 4) then we can have $k = x + y + 1/2 \cdot y \cdot (\sqrt{m} - 1) = x + 1/2 \cdot y + 1/2 \cdot y \cdot \sqrt{m}$ for x, y rational integers. In this case, $|(r - x - 1/2 \cdot y)^2 - m \cdot (s - 1/2 \cdot y)^2| = |N(\delta - k)| < 1$.

Theorem 9. *There are just five complex Euclidean quadratic fields. These are the fields in which m= -1, -2, -3, -7, -11.*

Proof: Let $m = -\mu < 0$. It suffices to show prove the inequalities

$$(1) \quad |(r-x)^2 - m \cdot (s-y)^2| = |(r-x)^2 + \mu \cdot (s-y)^2| < 1$$

for $m \neq 1(mod 4)$ and

$$(2) \quad |(r - x - 1/2 \cdot y)^2 - m \cdot (s - 1/2 \cdot y)^2| = |(r - x - 1/2 \cdot y)^2 + \mu \cdot (s - 1/2 \cdot y)^2| < 1$$

for $m = 1(mod 4)$ hold only in the fields for which m has the given values.

case 1. $m \neq 1(mod 4)$. In this case we need to show that inequality 1 holds only when $m = -1$, or $m = -2$. We take $r = 1/2$, $s = 1/2$ and $\delta = 1/2 + (1/2) \cdot \sqrt{m}$. If inequality 1 holds for this δ in $K(\sqrt{m})$ then $|((1/2) - x)^2 + \mu \cdot ((1/2) - y)^2| < 1$, or $|(1/4) + x \cdot (x-1) + \mu \cdot ((1/4) + y \cdot (y-1)| < 1$, but note that $x \cdot (x-1) \geq 0$, and $y \cdot (y-1) \geq 0$, so we have

$$1/4 + (1/4) \cdot \mu < |1/4 + x(x-1) + \mu(1/4 + y(y-1))| < 1$$

Hence, $\mu < 3$. Thus $\mu = 1$, or $\mu = 2$ are the only possible values. For these values if we take x, y to be the integers nearest to r, s respectively, we can plainly satisfy inequality 1.

case 2. $m = 1(mod 4)$. In this case we need to show that inequality 2 holds only when $m = -3$, or $m = -7$, or $m = -11$. We take $r = 1/4$, $s = 1/4$ and $\delta = 1/4 + (1/4) \cdot \sqrt{m}$. If inequality 2 holds for this δ in $K(\sqrt{m})$ then

$$|((1/4) - (x + (1/2)y))^2 + \mu(1/4 - (1/2)y)^2| < 1$$

or

$$|1/16 - 1/2 \cdot (x + 1/2 \cdot y) + (x + 1/2 \cdot y)^2 + \mu(1/16_1/4 \cdot y + 1/4 \cdot y^2)| < 1$$

or

$$|1/16 + (x + 1/2 \cdot y)(x + 1/2 \cdot y - 1/2) + \mu(1/16 + 1/4 \cdot y(y-1))| < 1$$

But the left hand side of the last inequality is greater than $1/16+1/16\cdot\mu$. Hence, $\mu < 15$. Since $\mu = 3(mod4)$, the only possible values of μ are 3, 7, 11. Now, given s there is a y such that $|2s - y| \leq 1/2$ and an x for which $|r - x - 1/2 \cdot y| \leq 1/2$ Then,

$$|(r - x - 1/2 \cdot y)^2 + \mu(s - 1/2 \cdot y)^2| \leq 1/4 + 11/16 = 15/16 < 1$$

Thus inequality 2 is satisfied when $m = -3, -7, -11$.

There are other simple fields such as $(\sqrt{-19})$ which are not Euclidean. The fields in which $m = -1, -2, -3, -7, -11, -19, -43, -67$, or -163 are simple. Heilbronn and Linfoot proved that there is at most one more. Lehmer has proved that for this field, if it exists, $m < -5 \cdot 10^9$; but its existence is highly improbable. (In fact, H. Stark showed that there is no other.)

The real Euclidean quadratic fields are more numerous, but the number of such fields are finite and they are completely determined by the following result.

Theorem 10. *$K(\sqrt{m})$ is Euclidean when m = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73 and for no other positive m.*

We shall prove that $K(\sqrt{m})$ is Euclidean when $m = 2, 3, 5, 6, 7, 13, 17, 21, 29$. Let's combine inequality 1 and inequality 2 to treat the two cases $(m = 1(mod4), m \neq 1(mod4))$ together. To accomplish this we do the following. Let, $\lambda = 0$ and n=m when $m \neq 1(mod4)$ and $\lambda = 1/2$ and $n = (1/4) \cdot m$ when $m = 1(mod4)$. Now if we replace $2s$ by s when $m = 1(mod4)$, then the two inequalities can be combined, and we get $|(r - x - \lambda \cdot y)^2 - n(s - y)^2| < 1|$. We refer to this inequality as inequality 3. Let's assume that $K(\sqrt{m})$ is not Euclidean. Then there exist some rationals r, s for which the inequality 3 is not true for all integral x, y.

We may assume that $0 \leq r, s \leq 1/2$ (inequality 4). This is easily seen when $m \neq 1(mod4)$. In this case inequality 3 is $|(r-x)^2 - m(s-y)^2| < 1|$ The value of the left hand side of this inequality remains unchanged if we replace r, x, s, y by $e_1 \cdot r + u$, $e_2 \cdot x + u$, $e_2 \cdot s + v$, $e_2 \cdot y + v$ respectively, where e_1, e_2 are each 1 or -1. we can choose e_1, e_2, u, v so that $e_1 \cdot r + u$, $e_2 \cdot s + v$ lie between 0 and 1/2 inclusive. In the case $m = 1(mod4)$, the inequality 3 becomes $|(r - x - (1/2) \cdot y)^2 - (1/4) \cdot (s - y)^2| < 1|$. The left hand side here is unaltered by the following substitutions:

$$1. e_1 \cdot r + u, e_1 \cdot x + u, e_1 \cdot s, e_1 \cdot y$$

$$2. r, x - v, s + 2 \cdot v, y + 2 \cdot v$$

$$3. r, x + y, -s, -y$$

$$4. 1/2 - r, -x, 1 - s, 1 - y$$

for r, x, s, y respectively.

We use 1 to make $0 \leq r \leq 1/2$; then 2 to make $-1 \leq s \leq 1$. if $-1 \leq s \leq 0$, then 3 makes $0 \leq s \leq 1$. If yet s does not lie between 0 and 1/2 inclusive, we use 4 to make s to lie between 0 and 1/2. Now we let, $P(x, y)$ be the inequality $(r - x - \lambda \cdot y)^2 \geq 1 + n(s - y)^2$ and let $Q(x, y)$ be inequality $n(s - y)^2 \geq 1 + (r - x - \lambda \cdot y)^2$. There are therefore some rationals r, s satisfying inequality 4 such that one or the other of $P(x, y)$, $Q(x, y)$ is true for all integral x, y. Consider The following.

$$\begin{array}{lll} P(0,0): & r^2 \geq 1 + ns^2 & Q(0,0): ns^2 \geq 1 + r^2 \\ P(1,0): & (1-r)^2 \geq 1 + ns^2 & Q(1,0): ns^2 \geq 1 + (1-r)^2 \\ P(-1,0): & (1+r)^2 \geq 1 + ns^2 & Q(-1,0): ns^2 \geq 1 + (1+r)^2 \end{array}$$

Note that r and s both can't be zero because if they are, both $P(0, 0)$ and $Q(0, 0)$ will be false. So r and s are not both 0. Then $P(0, 0)$, $P(1, 0)$ are both false; so $Q(0, 0)$, and $Q(1, 0)$ are true. If $P(-1, 0)$ were true then $P(-1, 0)$ together with $P(1, 0)$ implies that

$$(1 + r)^2 \geq 1 + n \cdot s^2 \geq 1 + (1 + (1 - r)^2)$$

and so $4 \cdot r \geq 2$. thus $r = 1/2$. But this will imply that $ns^2 = 5/4$. If $s = p/q$, where $\gcd(p, q) = 1$, then $4np^2 = 5q^2$. If $m \neq 1(mod4)$ then $n = m$, and so $4mp^2 = 5q^2$. Hence, $p = 1$ and $q = 2$. Therefore $s = 1/2$ and $m = 5$, a contradiction to $m \neq 1(mod4)$.

On the other hand, if $m = 1(mod4)$, then $m = 4n$, and so $mp^2 = 5q^2$. Hence $p = 1$, and $q = 1$. Therefore $s = 1$, a contradiction to inequality 4.

We conclude that $P(-1, 0)$ can't be true. So we have that $Q(-1, 0)$ is true. This gives us

$$ns^2 \geq 1 + (1 + r)^2 \geq 2$$

implying $n \geq 8$ using inequality 4. It now follows that there is an algorithm in all cases in which $n < 8$. These cases are $m = 2, 3, 5, 6, 7, 13, 17, 21, 29$.

A note on the proof: Notice that for $Q(x, y)$ to be true for all integral x, y, n should be a big number. On the other hand, for $P(x, y)$ to be true for all integral x, y, n should not be so big. Since, we have used only a finite number of values of x, y, we can't say that the values we've got for m, which is not the full list of theorem 10, are the only values.

Everything that we have said so far has been about algebraic numbers. There are numbers which are not algebraic. A number which is not algebraic is called transcendental. Since the set of integral polynomials is enumerable, the set of algebraic numbers is enumerable too. So we can say that almost all real numbers are transcendental because the set of real numbers is not enumerable, and in particular the set $\{x \epsilon R : 0 \leq x < 1\}$ is not enumerable. We conclude this paper by proving that e is transcendental.

We introduce a symbol h^r, which is defined by

$$h^0 = 1, h^r = r!(r \geq 1)$$

If $f(x) = \sum_0^m c_r \cdot x^r$ is any polynomial in x of degree m, then we define $f(h)$ as

$$\sum_0^m c_r \cdot h^r = \sum_0^m c_r \cdot r!$$

where $0! = 1$, and define $f(x + h)$ as

$$\sum_0^m (f^(r)(x)/r!)h^r = \sum_0^m f^(r)(x)$$

If we fix x, and let $F(y) = f(x + y)$, then $F(h) = f(x + h)$. We define $U_r(x)$ and $E_r(x)$, for $r = 0, 1, 2, \ldots$ by

$$\frac{U_r(x) = x \; over (r + 1) + (X^2)}{(r + 1)(r + 2) + \cdots = e^{|x|} \cdot E_r(x)}$$

We note that $|U_r(x)| < e^|x|$, and so $E_r(x) < 1$ for all x.

Lemma 1. *If $f(x) = \sum_0^n c_r \cdot x^r$ is any polynomial in x of degree n, and $g(x) = \sum_0^n c_r \cdot E_r(x) \cdot x^r$, then $e^x \cdot f(h) = f(x + h) + g(x)e^{|x|}$.*

Proof. We first show that $(x + h)^r = e^x \cdot h^r - U_r(x) \cdot x^r$.

$$\begin{aligned}
(x + h)^r &= h^r + r \cdot h^(r - 1) \cdot x + (r \cdot (r - 1)/2!) \cdot h^(r - 2) \cdot x^2 + \cdots + x^r \\
&= r! + r \cdot (r - 1)! \cdot x + r \cdot (r - 1) \cdot (r - 2)! \cdot x^2 + \cdots + x^r \\
&= r!(1 + x + x^2/2! + \cdots + x^r/r!) \\
&= r!(e^x - U_r(x) \cdot x^r \cdot (1/r!)) \\
&= r!e^x - U_r(x) \cdot x^r
\end{aligned}$$

so $e^x \cdot h^r = (x + h)^r + U_r(x) \cdot x^r$. Multiplying both sides by c_r and summing, we get

$$e^x \cdot f(h) = f(x + h) + e^|x| \cdot g(x)$$

Lemma 2. *Let $f(x)$ be any integral polynomial in x. If $m \geq 2$, and*

$$F_1(x) = \frac{< x^{(}m-1) >}{< (m-1)! >} \cdot f(x)$$

$$F_1(x) = \frac{< x^m >}{< (m-1)! >} \cdot f(x)$$

then $F_1(h)$ and $F_2(h)$ are both integers and $F_1(h) = f(0)(modm)$, and $F_2(h) = 0(modm)$.

proof. Let $f(x) = \sum_0^n b_r \cdot x^r$, where $a_1, a_2, \cdots, a_n$ are integers. Then,

$$F_1(x) = \sum_0^n \frac{b_r}{(m-1)!} \cdot x^{(}r+m-1)$$

and

$$F_2(x) = \sum_0^n \frac{b_r}{(m-1)!} \cdot x^{r+m}$$

So

$$\begin{aligned} F_1(h) &= \sum_0^n \tfrac{b_r}{(m-1)!} \cdot h^{(}r+m-1) \\ &= \sum_0^n \tfrac{b_r}{(m-1)!} \cdot (r+m-1)! \\ &= \sum_0^n b_r \cdot \tfrac{(r+m-1)!}{(m-1)!} \end{aligned}$$

which is an integer. When $r \geq 1$, $\frac{(r+m-1)!}{(m-1)!}$ is a multiple of m. Hence, we have $F_1(h) = f(0)(modm)$.

Similarly,

$$\begin{aligned} F_2(h) &= \sum_0^n \tfrac{b_r}{(m-1)!} \cdot h^{(}r+m) \\ &= \sum_0^n \tfrac{b_r}{(m-1)!} \cdot (r+m)! \\ &= \sum_0^n b_r \cdot \tfrac{(r+m)!}{(m-1)!} \end{aligned}$$

which is an integer. When $r \geq 0$, $\frac{(r+m)!}{(m-1)!}$ is a multiple of m. Hence, we have that $F_2(h) = 0(modm)$.

Theorem 11. *e is transcendental.*

proof. Suppose, on the contrary, that e is not transcendental. Then we can have

$$\sum_0^n a_t \cdot e^t = 0 \qquad (eq.1)$$

where $a_0, a_1, \cdots$ are integers, $a_0 \neq 0$, and $n \geq 1$. Let p be a prime which is greater than $\max(n, |a_0|)$, and

$$F(x) = (x-1) \cdot (x-2) \cdot \cdots \cdot (x-n)^p$$

We define

$$f(x) = \frac{x^{p-1}}{(p-1)!} \cdot (x-1) \cdot (x-2) \cdot \cdots \cdot (x-n)^p$$

If we multiply both sides of equation 1 by $f(h)$, and use lemma 1, we get

$$\begin{aligned} \textstyle\sum_0^n a_t \cdot f(h)e^t &= \textstyle\sum_0^n a_t \cdot (f(t+h) + g(t) \cdot e^t) \\ &= \textstyle\sum_0^n a_t \cdot f(t+h) + \sum_0^n a_t \cdot g(t) \cdot e^t \\ &= S_1 + S_2 \\ &= 0 \end{aligned}$$

By lemma 2, $f(h)$ is an integer and

$$f(h) = F(0)(modp) = (-1)^{n \cdot p} \cdot (n!)^p (modp)$$

For $1 \leq t \leq n$,

$$f(t+x) = \frac{(t+x)^{p-1}}{(p-1)!} \cdot (t+x-1) \cdot (t+x-2) \cdot \cdots x \cdot (x-1) \cdot \cdots (x+t-n)^p$$

$$= x^p \ over (p-1)! \cdot h(x)$$

for some integral polynomial $h(x)$ in x.

Again if we use lemma 2, it follows that $f(t+h)$ is an integer and $f(t+h) = 0(modp)$. So,

$$S_1 = \sum_0^n a_t \cdot f(t+h) = a_0 \cdot f(h)(modp) = (-1)^{n \cdot p} \cdot (n!)^p \cdot a_0(modp)$$

Since $a_0 \neq 0$, and $p > n, |a_0|$, $S_1 \neq 0(modp)$. Thus S_1 is an integer, and therefore $|S_1| \geq 1$.

Now we will show that $|S_2| < \frac{1}{2}$. To do this, we recall that $|E_r(x)| < 1$. We then have the following.

$$\begin{array}{rcc} |g(t)| & = & \sum_0^s |c_r| \cdot t^r \cdot |E_r(t)| \\ & < & \sum_0^s |c_r| \cdot t^r \cdot \\ & = & |f(t)| \\ & = & |\frac{t^{p-1}}{(p-1)!} \cdot (t-1) \cdot (t-2) \cdots (t-n)^p| \\ & \leq & \frac{x^{p-1}}{(p-1)!} \cdot (t+1) \cdot (t+2) \cdots (t+n)^p \end{array}$$

Hence, we can make $g(t)$ close to 0 by choosing p big enough. So we can get $|S_2| < \frac{1}{2}$ by choosing big enough. Since $|S_1| \geq 1$, and $|S_2| < \frac{1}{2}$, $S_1 + S_2$ cannot be equal to 0, which is a contradiction. We conclude that e is transcendental.

Some other examples of transcendental numbers known are π, $sin(1)$, $\log 2$, e^π.