

**From Studying Mathematics
to Doing Researches in Mathematics**

Jing Yu

NCTS and NTHU

November 2007, at National Taiwan Normal University

Factorization of polynomials in $\mathbb{Z}[X]$:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Getting degree one factors, and finding rational roots.

How to obtain factors with degree > 1 ?

Looking for Algorithms. L. Kronecker.

Suppose $g(X) = b^m X^m + \cdots + b_0$ and $g(X) | f(X)$.

May assume $m = \lfloor n/2 \rfloor$ and $f(X)$ without rational roots. Then for the non-zero integer values :

$$g(0) | f(0), \quad g(1) | f(1), \dots, \quad g(m) | f(m), \dots$$

Since $f(0), f(1), \dots, f(m)$ are fixed integers, and one knows how to factorize integers. There are only

finitely many possibilities for the set:

$$\{g(0), g(1), \dots, g(m)\}.$$

For each such possibility, there is at most one polynomial $g(X)$ taking these values at the $m + 1$ distinct integers $0, 1, \dots, m$. Solving the linear systems with coefficients of $g(X)$ as variables, or using Lagrange interpolation, one obtains such a polynomial in $\mathbb{Q}[X]$. If this happens to be a polynomial in $\mathbb{Z}[X]$ it is what we are looking for. Otherwise $f(X)$ must be irreducible as a polynomial with integral coefficients.

Lagrange interpolation : Suppose $g(X)$ having degree m and taking values c_i at distinct points b_i , $i = 0, \dots, m$. Then

$$g(X) = \sum_{i=0}^m c_i \frac{(X - b_0) \cdots \widehat{(X - b_i)} \cdots (X - b_m)}{(b_i - b_0) \cdots (b_i - b_i) \cdots (b_i - b_m)}.$$

Rationalizing the denominator of an irrational.

$$\frac{1}{\sqrt[5]{8} + 1} = \frac{-2\sqrt[5]{16}}{9} + \frac{-\sqrt[5]{8}}{9} + \frac{4\sqrt[5]{4}}{9} + \frac{2\sqrt[5]{2}}{9} + \frac{1}{9}.$$

Let α be root of an irreducible polynomial $f(x) \in \mathbb{Q}[X]$. Let $g(X)$ be another polynomial in $\mathbb{Q}[X]$ relative prime to $f(X)$. **Compute** $1/g(\alpha)$.

Euclidean Algorithm: Compute $r(X), s(X) \in \mathbb{Q}[X]$ satisfying $r(X)f(X) + s(X)g(X) = 1$. Then

$$s(\alpha) = 1/g(\alpha).$$

Solving system of (non-linear) polynomial equations.

$$\begin{cases} x^2 - y^2 = 1 \\ x^2 + y^2 = 3 \end{cases}$$

How to find the solution set if it is finite?

How to describe the solution set if it is infinite?

What are the **Algorithms** for solving such systems?

Extending **Gauss elimination** method to non-linear systems?

Extending **Division Algorithm** to polynomials in several variables?

Ordering monomials in several variables, and passing from given system to equivalent systems.

Manipulating symbols and simplifying mathematical expressions.

Inverting polynomial maps. Consider

$$F : \mathbb{C}^n \longrightarrow \mathbb{C}^n,$$

$$y_1 = f_1(x_1, \dots, x_n)$$

$$y_2 = f_2(x_1, \dots, x_n)$$

$$\vdots$$

$$y_n = f_n(x_1, \dots, x_n)$$

where $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$.

Determining whether there is polynomial map G on \mathbb{C}^n such that $F \circ G = G \circ F = \text{Id}$.

Find the inverse $G = (g_1, \dots, g_n)$ in case it exists.

The linear map case, **Determinant**.

Algorithm for inverting polynomial maps.

Power Sums :

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4},$$

$$1^k + 2^k + \cdots + n^k = S_k(n)?$$

Is $S_k(n)$ always a polynomial in n ? i.e.

$S_k(X) \in \mathbb{Q}[X]$? What are their degrees? What are their leading terms? ($X^{k+1}/(k+1)$)

A **formula** for all positive integers k , and n .

J. Bernoulli and L. Euler. Method of **generating functions**. Consider **formal power series** :

$$\sum_{k=0}^{\infty} S_k(n) \frac{Z^k}{k!},$$

here Z is an independent **variable**. Then

$$\frac{e^{(n+1)Z} - 1}{e^Z - 1} = \sum_{k=0}^{\infty} S_k(n) \frac{Z^k}{k!}.$$

Here e^Z is the well-known exponential function.

$$e^Z = \sum_{m=0}^{\infty} \frac{Z^m}{m!}.$$

Expanding and comparing coefficients of formal power series on both sides gives desired formulas for $S_k(n)$.

Following rational B_m called **Bernoulli numbers**:

$$\frac{z}{e^z - 1} = \sum_{m=0}^{\infty} B_m \frac{z^m}{m!}.$$

Searching for proofs of the **Fundamental Theorem** of Algebra. Knowing special cases, e.g. the Quadratic case, De Moivre Theorem, Intermediate value Theorem for polynomials, etc.

Greek geometric constructions with ruler and compass. The Three Problems: trisect arbitrary given angle, doubling the cube, and squaring the circle. The concept of “Insolvability”. Cartesian coordinates. Introducing field extensions. Extensions of \mathbb{Q} with degree which are powers of 2. Geometric construction of regular n -gons, legends of Gauss, Fermat.

Finding **roots of polynomial equation** via coefficients of the given polynomial.

Formulas for quadratic equations $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Formulas for cubic equations?

Formulas for quartic equations?

Searching for formulas for general equations of degree 5 or more. Introducing **groups**.

Solvability by Radicals. Legends of Abel, Galois.

Differentiation and integration.

Fundamental theorem of calculus.

Indefinite integrals for **elementary functions**.

Looking for “antiderivatives”, e.g.

$$\int \frac{dx}{\sqrt{1-x^3}} = ?$$

A “closed” formula, i.e. a finite expressions in terms

of elementary functions.

$$\int \frac{dx}{\sqrt{1-x^2}} = \arcsin x.$$

Determining whether the indefinite integral of a given elementary function is elementary?

Looking for **algorithms** to do integration.

Field of functions, e.g. field of rational functions in one variable $\mathbb{R}(x)$.

Partial fractions decomposition as a tool in calculus.

The concept a field F with a derivation $D : F \rightarrow F$ which satisfies the Leibnitz rule : for all $f, g \in F$

$$D(f \cdot g) = Df \cdot g + f \cdot Dg.$$

Exponentials and logarithms for differential fields :

Call g the exponential of f if $Dg = g \cdot Df$,

Call g the logarithm of f if $Dg = \frac{Df}{f}$.

Consider elementary extensions of differential fields.

Reciprocal power sums. Prove:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90},$$

These infinite sums are rational multiples of “right” powers of π . Euler proved for all positive **even** $2m$

$$\zeta(2m) = \sum_{n=1}^{\infty} \frac{1}{n^{2m}} = \frac{-(2\pi\sqrt{-1})^{2m} B_{2m}}{2(2m)!}.$$

Both the power sums and the reciprocal **even** power sums are connected with the Bernoulli numbers:

$$B_1 = -1/2, B_2 = -1/6, B_3 = 0, B_4 = -1/30, B_5 = 0,$$

$$B_6 = 1/42, B_7 = 0, B_8 = -1/30, B_9 = 0, B_{10} = 5/66 \dots$$

$$\sum_{n=1}^{\infty} \frac{1}{n^3} = \zeta(3) = ?$$

1978 Apéry $\zeta(3)$ irrational. Transcendental? Let

$$S = \{\pi, \zeta(2), \zeta(3), \dots, \zeta(m) \dots\}$$

Conjecture all the values $\zeta(m)$ for integer $m > 1$ should be transcendental, moreover the Euler-Bernoulli relations generate all the algebraic relations among numbers from S over the field of algebraic numbers. In particular, all the values $\zeta(m)$ for odd integer $m > 1$ should be algebraically independent from each other, as well as algebraically independent from π .

The Riemann zeta function.

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \operatorname{Re}(s) > 1 \\ &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},\end{aligned}$$

by the unique factorization of integers.

Values $\zeta(s)$ at integers $s \leq 1$? Analytic continuation.

Symmetry between $\zeta(s)$ and $\zeta(1 - s)$.

Riemann Hypothesis.

In the world of positive characteristic p , let θ be a variable over finite field \mathbb{F}_q .

For reciprocal power sums one considers, $m \geq 1$,

$$\zeta_C(m) = \sum_{\substack{a \in \mathbb{F}_q[\theta] \\ a \text{ monic}}} \frac{1}{a^m} \in \mathbb{F}_q\left(\left(\frac{1}{\theta}\right)\right),$$

Here $\mathbb{F}_q\left(\left(\frac{1}{\theta}\right)\right)$ is the field of formal Laurent series.

One has the obvious Frobenius relations among these Carlitz zeta values for all positive integer m :

$$\zeta_C(m)^p = \zeta_C(mp).$$

If m is **even**, i.e. $m \equiv 0 \pmod{q-1}$

because the ring $\mathbb{F}_q[\theta]$ has $q - 1$ signs,
the Euler-Carlitz relation says

$$\zeta_C(m) = \frac{\tilde{\pi}^m \tilde{B}_m}{\Gamma_{m+1}},$$

where $\tilde{\pi}$ is a fundamental period of Carlitz :

$$\tilde{\pi} = \theta(-\theta)^{\frac{1}{q-1}} \prod_{i=1}^{\infty} \left(1 - \theta^{1-q^i}\right)^{-1},$$

which is transcendental over $\mathbb{F}_q(\theta)$.

The Γ_m are the Carlitz factorials for $\mathbb{F}_q[\theta]$:

(i) setting $D_0 = 1$, and for $i \geq 1$

$$D_i = (\theta^{q^i} - \theta^{q^{i-1}}) \cdots (\theta^{q^i} - \theta),$$

(ii) writing down the q -adic expansion $\sum_{i=0}^{\infty} n_i q^i$ of n ,

and let

$$\Gamma_{n+1} = \prod_{i=0}^{\infty} D_i^{n_i}.$$

The $\widetilde{B}_m \in \mathbb{F}_q(\theta)$ are Bernoulli-Carlitz “numbers” given by

$$\frac{z}{\exp_C(z)} = \sum_{m=0}^{\infty} \widetilde{B}_m \frac{z^m}{\Gamma_{m+1}}.$$

Here Carlitz exponential $\exp_C(z)$ is the series

$$\exp_C(z) = \sum_{h=0}^{\infty} \frac{z^{q^h}}{D_h} = z \prod_{\substack{a \in \mathbb{F}_q[\theta] \\ a \neq 0}} \left(1 - \frac{z}{a\tilde{\pi}}\right).$$

We are interested in the following values from arithmetic of $\mathbb{F}_q(\theta)$:

$$S_q = \{\tilde{\pi}, \zeta_C(1), \zeta_C(2), \dots, \zeta_C(m) \dots\}$$

All these values are transcendental over $\bar{k} = \overline{\mathbb{F}_q(\theta)}$.

Transcendence of $\zeta_C(n)$ when $n \not\equiv 0 \pmod{q}$,

J. Yu 1991, Annals of Mathematics.

C.-Y. Chang, J. Yu 2007, Advances in Mathematics, proves that the Euler-Carlitz relations and the Frobenius relations generate all the algebraic relations among elements from S_q over the field of algebraic functions \bar{k} . Thus the transcendence degree of the set $S^{(n)} = \{\tilde{\pi}, \zeta_C(1), \dots, \zeta_C(n)\}$ is exactly

$$n - \lfloor n/p \rfloor - \lfloor n/(q-1) \rfloor + \lfloor n/(p(q-1)) \rfloor + 1.$$