IRREDUCIBILITY OF TRUNCATED EXPONENTIALS

KEITH CONRAD

We will use algebraic number theory (prime ideal factorizations) to prove the irreducibility in $\mathbf{Q}[X]$ of each truncated exponential series

$$1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$$

where $n \geq 1$. In fact, we will prove more than this.

Theorem 1 (Schur, 1929)**.** *Any polynomial*

$$1 + c_1 X + c_2 \frac{X^2}{2!} + \cdots + c_{n-1}\frac{X^{n-1}}{(n-1)!} \pm \frac{X^n}{n!}$$

with $c_i \in \mathbf{Z}$ is irreducible in $\mathbf{Q}[X]$.

We can't let the constant term be a general integer. For example, $c_0 + X + \frac{1}{2}X^2$ is reducible when $c_0 = -2b(b+1)$ for $b \in \mathbf{Z}$.

The proof of Theorem 1 will require an extension of Bertrand's Postulate. In its original form, conjectured by Bertrand and proved by Chebyshev, the "postulate" says that for every positive integer k there is a prime number p satisfying $k < p \leq 2k$. Here is a generalization.

Lemma 2. *The product of k consecutive integers that are all greater than k contains a prime factor that is greater than k. That is, for positive integers $k \leq \ell$, at least one of the numbers in the list*

$$\ell + 1, \ell + 2, \ldots, \ell + k$$

is divisible by a prime number $> k$.

Proof. This was independently proved by Schur [3] and Sylvester [6], and later reproved by Erdos [2]. □

When $k = \ell$ this lemma says some number from $k+1$ to $2k$ is divisible by a prime $> k$. In that range, a number divisible by a prime $> k$ is prime, so Bertrand's postulate is a special case of Lemma 2.

Now we prove Theorem 1.

Proof. Multiply the polynomial by $n!$ to clear denominators: set

$$F(X) = \sum_{i=0}^{n} \frac{n!}{i!} c_i X^i = \pm X^n + nc_{n-1}X^{n-1} + \cdots + n!c_1 X + n!.$$

To prove $F(X)$ is irreducible in $\mathbf{Q}[X]$, we will assume it is reducible and get a contradiction by investigating the prime ideal factorization of each coefficient of $F(X)$ in the number field generated by a suitable root of $F(X)$.

Since $F(X)$ is in $\mathbf{Z}[X]$ with leading coefficient ± 1, it has to have an irreducible monic factor $A(X) \in \mathbf{Z}[X]$ of degree $m \leq n/2$. Write

$$A(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0.$$

Step 1: We show each prime factor of $\frac{n!}{(n-m)!} = n(n-1)\cdots(n-m+1)$ divides a_0. This will just be some algebra, no algebraic number theory.

Let p be a prime factor of $\frac{n!}{(n-m)!}$. For $0 \leq i \leq n-m$, the coefficient of X^i in $F(X)$ is a multiple of $\frac{n!}{i!}$, and $\frac{n!}{i!}$ is divisible by p. Therefore $F(X) \bmod p$ is divisible by X^{n-m+1}.

Write $F(X) = A(X)B(X)$, so $B(X)$ has degree $n-m$ in $\mathbf{Z}[X]$ with leading coefficient ± 1. Reducing mod p, $X^{n-m+1} \mid \overline{A}(X)\overline{B}(X)$ in $\mathbf{F}_p[X]$. Since $\overline{B}(X)$ has degree $n-m$, we must have $X \mid \overline{A}(X)$. This means the constant term $\overline{A}(0)$ is 0, which means $p \mid a_0$.

Step 2: Each prime factor of a_0 is $\leq m$.

Let p be a prime factor of a_0 and let α be a root of $A(X)$. Set $K = \mathbf{Q}(\alpha)$, so $[K : \mathbf{Q}] = m$. Since $A(X)$ is monic in $\mathbf{Z}[X]$, $\alpha \in \mathcal{O}_K$. Its norm down to $\mathbf{Q}$ is

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \pm a_0 \equiv 0 \bmod p.$$

Since the ideal (α) in $\mathcal{O}_K$ has norm $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$, which is divisible by p, some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ lying over p divides (α). Pull out the largest powers of $\mathfrak{p}$ from (α) and (p):

$$(\alpha) = \mathfrak{p}^d\mathfrak{a}, \quad (p) = \mathfrak{p}^e\mathfrak{b},$$

where d and e are positive integers and $\mathfrak{a}$ and $\mathfrak{b}$ are not divisible by $\mathfrak{p}$. Note $e = e(\mathfrak{p}|p) \leq m$.

Since $F(\alpha) = 0$,

$$0 = \pm\alpha^n + nc_{n-1}\alpha^{n-1} + \cdots + n!c_1\alpha + n!,$$

so

$$-n! = \pm\alpha^n + nc_{n-1}\alpha^{n-1} + \cdots + n!c_1\alpha = \pm\alpha^n + \sum_{i=1}^{n-1} \frac{n!}{i!}c_i\alpha^i. \tag{0.1}$$

We will look at the highest power of p and $\mathfrak{p}$ in factorials. For a positive integer r, Legendre showed the highest power of p dividing $r!$ is

$$s_r := \sum_{j\geq 1}\left[\frac{r}{p^j}\right] < \frac{r}{p-1}.$$

Therefore $\mathrm{ord}_{\mathfrak{p}}(r!) = e\,\mathrm{ord}_p(r!) = es_r$. The left side of (0.1) is $n!$, which has $\mathfrak{p}$-adic valuation es_n, so at least one of the terms on the right side of (0.1) has $\mathfrak{p}$-adic valuation $\leq es_n$. That is, for some i from 1 to n (where we set $c_n = \pm 1$), $c_i \neq 0$ and

$$\mathrm{ord}_{\mathfrak{p}}\left(\frac{n!}{i!}c_i\alpha^i\right) \leq es_n.$$

Since

$$\mathrm{ord}_{\mathfrak{p}}\left(\frac{n!}{i!}c_i\alpha^i\right) = es_n - es_i + \mathrm{ord}_{\mathfrak{p}}(c_i) + id \geq es_n - es_i + id,$$

we have $es_n - es_i + id \leq es_n$ for some i, so

$$id \leq es_i < e\frac{i}{p-1} \Longrightarrow (p-1)d < e \leq m \Longrightarrow p \leq m.$$

Step 1 tells us all the prime factors of the numbers from n down to $n-m+1$ divide a_0 and Step 2 tells us all these prime factors are at most m. So $n, n-1, \ldots, n-m+1$ is a list of m consecutive integers all greater than m that have no prime factor greater than m. This contradicts Lemma 2. $\square$

Corollary 3. *For all $n \geq 1$, the polynomials*

$$C_n(X) = 1 - \frac{X^2}{2!} + \cdots + (-1)^n\frac{X^{2n}}{(2n)!},$$

which are truncations of the power series for $\cos X$, are irreducible in $\mathbf{Q}[X]$.

Corollary 4. *For all $n \geq 0$, the polynomials*

$$1 + X - \frac{X^3}{3!} + \cdots + (-1)^n \frac{X^{2n+1}}{(2n+1)!}$$

and

$$1 - X + \frac{X^3}{3!} - \cdots + (-1)^{n-1} \frac{X^{2n+1}}{(2n+1)!},$$

which are truncations of the power series for $1 \pm \sin X$, are irreducible in $\mathbf{Q}[X]$.

Schur [4] used similar ideas to prove irreducibility over $\mathbf{Q}$ of the truncations of $e^X - 1$ and $\sin X$ after a factor of X is removed:

$$\frac{E_n(X) - 1}{X} = 1 + \frac{X}{2!} + \cdots + \frac{X^{n-1}}{n!},$$
$$\frac{S_n(X)}{X} = 1 - \frac{X^2}{3!} + \cdots + (-1)^n \frac{X^{2n}}{(2n+1)!}.$$

He proved more generally that polynomials of the form

$$1 + c_1 \frac{X}{2!} + c_2 \frac{X^2}{3!} + \cdots + c_{n-1} \frac{X^{n-1}}{n!} \pm \frac{X^n}{(n+1)!}$$

with $c_i \in \mathbf{Z}$ are irreducible over $\mathbf{Q}$ except perhaps if $n = 2^k - 1$ for $k \geq 2$ when it might be a product of $X \pm 2$ and an irreducible polynomial of degree $n - 1$, or $n = 8$ when it might be a product of irreducibles of degrees 2 and 6.

For the truncated exponential polynomial $E_n(X) = 1 + X + X^2/2! + \cdots + X^n/n!$, Schur showed its Galois group over $\mathbf{Q}$ is as large as possible: S_n when $n \not\equiv 0 \bmod 4$ and A_n when $n \equiv 0 \bmod 4$. (The discriminant of $E_n(X)$ is $(-1)^{n(n-1)/2} n!^n$, which is a square when $n \equiv 0 \bmod 4$ but not otherwise.) Coleman [1] reproved the irreducibility of $E_n(X)$ and the computation of its Galois group over $\mathbf{Q}$ using Newton polygons and Bertrand's postulate (not the more general Lemma 2), but this doesn't prove the irreducibility of the general polynomials in Theorem 1.

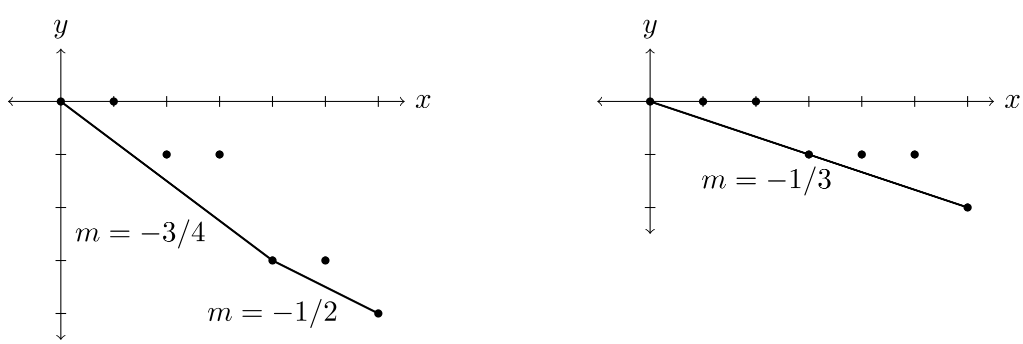

FIGURE 1. The 2-adic and 3-adic Newton polygon of $E_6(X)$,

Figure 1 is the 2-adic and 3-adic Newton polygons of $E_6(X)$, and Figures 2 and 3 are the 2-adic and 3-adic Newton polygons of $E_{12}(X)$. Coleman's basic observation is that for each prime p dividing n, the different slopes of the p-adic Newton polygon of $E_n(X)$ are fractions whose denominator (in reduced form) is divisible by the highest power of p

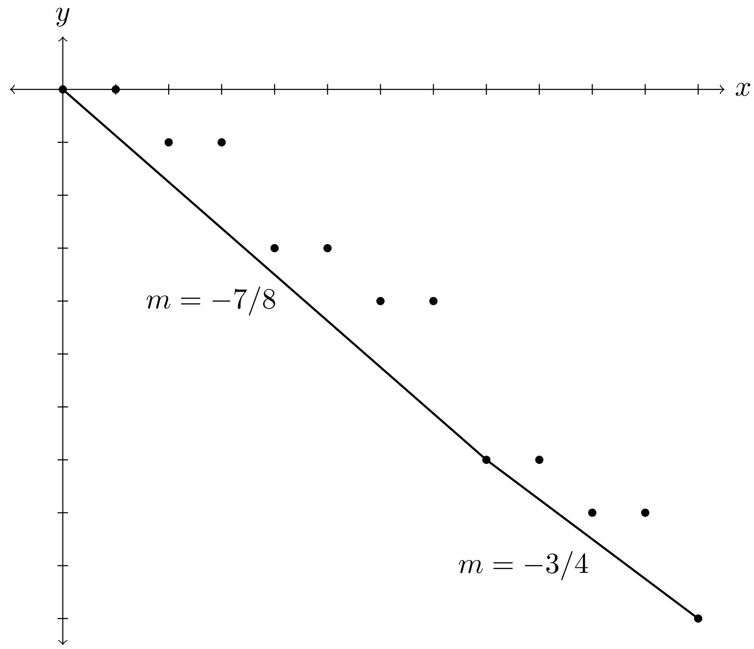

FIGURE 2. The 2-adic Newton polygon of $E_{12}(X)$.

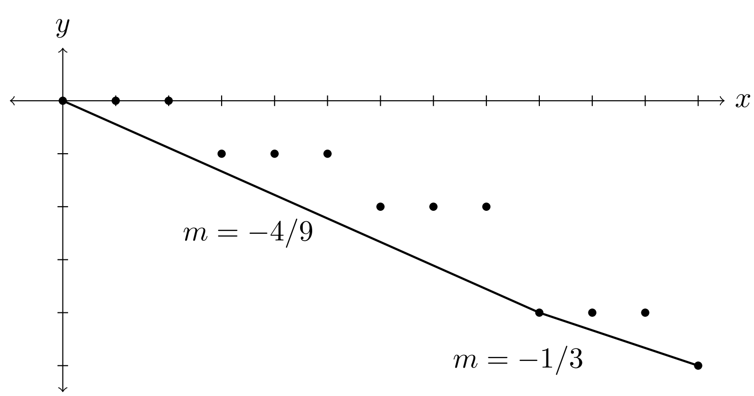

FIGURE 3. The 3-adic Newton polygon of $E_{12}(X)$.

dividing n, say p^{n_p}.[1] The connection between Newton polygons and p-adic valuations of roots of polynomials tells us that the irreducible factors of $E_n(X)$ in $\mathbf{Q}_p[X]$ have degree divisible by p^{n_p}. An irreducible factor $f(X)$ of $E_n(X)$ in $\mathbf{Q}[X]$ is a product of irreducible factors of $E_n(X)$ in $\mathbf{Q}_p[X]$, so $f(X)$ is a product of polynomials in $\mathbf{Q}_p[X]$ whose degrees are each divisible by p^{n_p}. Thus $p^{n_p} \mid \deg f(X)$ for each p dividing n. Letting p run over the prime factors of n, we get $n \mid \deg f(X)$. Since $E_n(X)$ has degree n, $E_n(X)$ is irreducible in $\mathbf{Q}[X]$.

[1]More precisely, the denominators of the slopes are the different powers of p that appear in the base p expansion of n, *e.g.*, the base 2 and base 3 expansions $6 = 2 + 4 = 2 \cdot 3$ are related to the denominators 2, 4, and 3 of the slopes in Figure 1.

References

[1] R. Coleman, On the Galois groups of the exponential Taylor polynomials, *Enseign. Math.* **33** (1987), 183–189.

[2] P. Erdos, A theorem of Sylvester and Schur, *J. London Math. Soc.* **9** (1934), 282–288.

[3] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I, *Sitzungsberichte Preuss. Akad. Wiss. Phys.-Math. Klasse* (1929), 125–136. Also in *Gesammelte Abhandlungen*, Band III, 140–151.

[4] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen II, *Sitzungsberichte Preuss. Akad. Wiss. Phys.-Math. Klasse* (1929), 370–391. Also in *Gesammelte Abhandlungen*, Band III, 152–173.

[5] I. Schur, Gleichungen ohne Affekt, *Sitzungsberichte Preuss. Akad. Wiss. Phys.-Math. Klasse* (1930), 443–449. Also in *Gesammelte Abhandlungen*, Band III, 191–197.

[6] J. Sylvester, On arithmetical series, *Messenger of Math.* **21** (1892), 1–19, 87-120. Also in *Mathematical Papers* **4** (1912), 687–731.