IRREDUCIBILITY OF TRUNCATED EXPONENTIALS

KEITH CONRAD

We will use algebraic number theory (just prime ideal factorizations) to prove the irreducibility in $\mathbf{Q}[X]$ of any 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 $c_0 = -2b(b+1)$.

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 any positive integer k there is a prime number p satisfying $k < p \leq 2k$. Here is a generalization.

Lemma 1. *The product of any k consecutive integers which 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 Sylvester [5] and Schur [3], 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 1.

Now we prove Theorem 1.

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

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

Assume $F(X)$ is reducible in $\mathbf{Q}[X]$. We will get a contradiction by investigating the prime ideal factorization of each coefficient of $F(X)$ in the number field generated by a 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.

Suppose p is a prime factor of $\frac{n!}{(n-m)!}$. For all $i \le n-m$, 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, $X^{n-m+1} | \overline{A}(X)\overline{B}(X)$ in $\mathbf{F}_p[X]$. Since $\overline{B}(X)$ has degree $n-m$, we must have $X | \overline{A}(X)$. This means the constant term $\overline{A}(0)$ is 0, which means $p | a_0$.

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

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

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

Passing to norms of ideals, $p | \mathrm{N}_{K/\mathbf{Q}}(\alpha) \Rightarrow p | \mathrm{N}((\alpha))$, so 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 $e = e(\mathfrak{p}|p) \le m$.

Since $F(\alpha) = 0$,

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

so

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

We will look at the highest power of primes in factorials. For any positive integer r, Legendre showed the highest power of p dividing $r!$ is

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

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

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

Since

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

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

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

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 which have no prime factor greater than m. This contradicts Lemma 1. $\square$

For the truncated exponential polynomial of degree n, Schur went further [4] and 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 the polynomial is $(-1)^{n(n-1)/2} n!^n$, which is a perfect square when $n \equiv 0 \bmod 4$ but not otherwise.) Coleman [1] reproved the irreducibility of the truncated exponential polynomials and the computation of their Galois groups using Newton polygons and Bertrand's postulate (not the more general Lemma 1), but this didn't recover the irreducibility of more general polynomials in Theorem 1.

Corollary 1. *For any $n \geq 1$, the truncated cosine series*

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

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

Schur used similar ideas to prove the irreducibility of the truncated sine series after a factor of X is removed:

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

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* **14** (1929), 125–136. Also in *Gesammelte Abhandlungen*, Band III, 140–151.

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

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