1
Prologue

In this chapter we give a couple of examples where the method of auxiliary polynomials is used for problems that have no diophantine character. Thus we are not following Sam Goldwyn's advice to start with an earthquake and work up to a climax.

Here is maybe one of the simplest examples.

There is an old chestnut which often turns up in problem-solving sessions: given a polynomial F in a variable X, can one always multiply it by a non-zero polynomial to get a product involving only powers X^p for p prime?

For example with $F = X^{100} + 1$ we have $X^3F = X^{103} + X^3$. But what about $F = X^{100} + X^3$? Here multiplying by some $P = aX^d$ will not do. However

$$(X^{111} - X^{14})F = X^{11}(X^{100} - X^3)F = X^{11}(X^{200} - X^6) = X^{211} - X^{17}.$$

At first sight it appears to be a difficult problem about primes, possibly in arithmetic progressions. So what about $F = X^{1000} + X^{100} + X^3$?

Let us consider multiplying F by some

$$P = \sum_{i=0}^{L} p_i X^i \tag{1.1}$$

for unknown L and undetermined coefficients p_i (not necessarily primes, but they might be). Then PF has degree at most $L + 1000$, and its coefficients are linear forms in the p_i. We would like to eliminate the terms X^n for n not prime with $0 \le n \le L + 1000$. There are

$$L + 1001 - \pi(L + 1000)$$

of these, where $\pi(x) = \sum_{p \le x} 1$ is the standard prime-counting function. If we equate the corresponding coefficients to zero, then we get a system of

$L+1001-\pi(L+1000)$ homogeneous linear equations in the $L+1$ unknowns p_i. By linear algebra this system is solvable non-trivially, provided

$$L+1 \ > \ L+1001-\pi(L+1000);$$

that is, $\pi(L+1000) > 1000$. Every schoolgirl knows that there are infinitely many prime numbers, so $\pi(x)$ tends to infinity with x and there exists such an L; for example $L = 6927$ (with Maple). So the answer is yes for this F; the trouble of course is that we have to solve 6927 equations in 6928 unknowns to get P explicitly.

The reader may now see first that this works for any F, and second that the primes are irrelevant, in the sense that we may demand only powers X^m in PF with m in any prescribed infinite set; for example the elements of the sequence $4, 27, 3125, 823543, \ldots$ of all $m = p^p$.

This is perhaps the simplest application of the method of auxiliary polynomials.

Here is a second example.

Consider the expressions

$$x = t^2 + t, \ \ y = t^2 + 1. \tag{1.2}$$

How can we eliminate t? Common sense, or a general consideration of transcendence degree, shows that there must be an algebraic relation between x, y not involving t. And indeed a moment's thought gives

$$x^2 - 2xy + y^2 + 2x - 3y + 2 = 0. \tag{1.3}$$

But what about

$$x = t^3 + t, \ \ y = t^4 + t?$$

We could solve the first equation by radicals for t, and then substitute into the second equation, and finally somehow clear the radicals. We get

$$x^4 + 3x^3 - 4x^2y - y^3 + 3x^2 - 5xy + 2y^2 + 2x - 2y = 0 \tag{1.4}$$

but I confess that here I just used Maple to calculate the resultant (see Chapter 5) of

$$t^3 + t - x, \ \ t^4 + t - y$$

with respect to t.

What about

$$x = t^{1948} + t^{666} + 1, \ \ y = t^{1291} + t^{163} + t? \tag{1.5}$$

Here the degrees are my year of birth and the (traditional) year of birth of the earliest part of the Swiss Federation, where I first gave these lectures

(in Basle, after earlier attempts in Ann Arbor, Constance, Hong Kong, Heraklion and Vienna).

Maple doesn't respond for 47 seconds; and then gives an incomprehensible error message (the resultant that you are seeking does not exist). How can we find this relation $P(x, y) = 0$?

Let us write

$$P(X, Y) = \sum_{i=0}^{L} \sum_{j=0}^{L} p_{ij} X^i Y^j \tag{1.6}$$

for unknown L and undetermined coefficients p_{ij} which are presumably integers as in (1.3) and (1.4). If we substitute (1.5) into $P(x, y)$, then we obtain a polynomial in t of degree at most $3239L$. Its coefficients are linear forms in the p_{ij}. If we equate these coefficients to zero, then we get a system of $3239L + 1$ homogeneous linear equations in the $(L + 1)^2$ unknowns p_{ij}. By linear algebra this system is solvable non-trivially, provided

$$(L + 1)^2 > 3239L + 1$$

for example if $L = 3238$.

This proves something: namely that there is a non-trivial relation of degree at most 3238 in each variable. There may well be $(L + 1)^2 = 10491121$ terms in the relation, which accounts for Maple's chickening out. And the trouble for anyone, of course, is that we now have to solve 10487883 equations in 10491121 unknowns.

The reader may see first that this works for any two polynomials F, G in t instead of (1.5), and second that it generalizes to more variables; for example between any three polynomials in two variables there is a non-trivial algebraic relation (as would follow more simply by consideration of transcendence degree).

This example is perhaps more typical of those to follow in these pages. After the substitution (1.5) we may regard the function $P(x, y)$ as having a large order of vanishing at $t = 0$; so large, indeed, that it must vanish identically.

In both examples the goal is practically the auxiliary polynomial itself; so it is hardly "auxiliary".

We will see many more and subtler applications in this book (sadly not Siegel's Theorem (Siegel, 1955) about functions on compact manifolds, which is a very sophisticated generalization of the second example – see however Lemma 20.4 and Exercise 20.67). But before we start, let us ask: since there appear to be so many terms in the relation connecting (1.5), what are the coefficients like? If we normalize them to be integers, how big are they? We note that the Cramér formulae for solving linear equations involve determinants

whose size is the number n of unknowns. Such determinants already have $n!$ terms, so their values are likely to be somewhat larger. Thus it would be surprising if the integers in our relation were substantially less than the factorial $10491121!$. And it can be seen that some of the entries of the determinants are almost as large as 3^{6476} (as in Exercise 1.17). This means that we could expect some coefficients in P to have thirty thousand million (American thirty billion, Swiss dreissig Milliarden) decimal digits (see however Exercise 8.13). So it is doubtful if P could ever be expressed explicitly.

Exercises

1.1 Show that there is $P \neq 0$ in $\mathbb{C}[X]$ such that $P(X)(X^{1000} + X^{100} + X^3)$ has the form $\sum_{n=0}^{N} a_n X^{n^2}$.

1.2 Let F be in $\mathbb{C}[X]$ with degree at most D. Show that there is $P \neq 0$ in $\mathbb{C}[X]$ with degree at most $D^2 - D$ such that PF has the form $\sum_{n=0}^{N} a_n X^{n^2}$.

1.3 Let F be in $\mathbb{C}[X]$. Find $P \neq 0$ in $\mathbb{C}[X]$ such that PF has the form $\sum_{n=0}^{N} a_n X^{2n}$.

1.4 Let F be in $\mathbb{C}[t]$ with degree at most $D \geq 1$ and let G be in $\mathbb{C}[t]$ with degree at most $E \geq 1$. Show that there is $P \neq 0$ in $\mathbb{C}[X, Y]$ with degree at most $D + E - 1$ in each variable such that $P(F, G) = 0$.

1.5 Let F be in $\mathbb{C}[t]$ with degree at most $D \geq 1$ and let G be in $\mathbb{C}[t]$ with degree at most $E \geq 1$. Show that there is $P \neq 0$ in $\mathbb{C}[X, Y]$ with degree at most E in X and degree at most $DE - E + 1$ in Y such that $P(F, G) = 0$.

1.6 Let t, u be independent variables, and let F, G, H be in $\mathbb{C}[t, u]$. Show that there is $P \neq 0$ in $\mathbb{C}[X, Y, Z]$ such that $P(F, G, H) = 0$.

* * * * * * * * * * * * * * * * * * *

1.7 Show that there is an absolute constant c (that is, not depending on any parameters) with the following property. Let F be in $\mathbb{C}[X]$ with degree at most $D \geq 2$. Then there is $P \neq 0$ in $\mathbb{C}[X]$ with degree at most $cD \log D$ such that PF has the form $\sum_p a_p X^p$, where p runs over the set of primes.

1.8 Let F be in $\mathbb{C}[X]$. Find $P \neq 0$ in $\mathbb{C}[X]$ such that PF has the form $\sum_{n=0}^{N} a_n X^{3n}$.

1.9 Let F be in $\mathbb{F}_p[X]$. Show that there is $P \neq 0$ in $\mathbb{F}_p[X]$ such that $G = PF$ satisfies $G(X_1 + X_2) = G(X_1) + G(X_2)$ in $\mathbb{F}_p[X_1, X_2]$.

1.10 Let F be in $\mathbb{C}[t]$ with degree at most $D \geq 1$ and let G be in $\mathbb{C}[t]$ with degree at most $E \geq 1$. Show that there is $P \neq 0$ in $\mathbb{C}[X, Y]$ with degree at most E in X and degree at most D in Y such that $P(F, G) = 0$ [*Hint*: resultants].

1.11 Let $P \neq 0$ in $\mathbb{C}[X, Y]$ be such that $P(t^{1948} + t^{666} + 1, t^{1291} + t^{163} + t) = 0$. Show that P has degree at least 1291 in X and degree at least 1948 in Y (compare Exercise 5.7).

1.12 Can one essentially improve the $D^2 - D$ in Exercise 1.2? I don't know.

1.13 Let F, G be in $\mathbb{C}(t)$ (rational functions). Show that there is $P \neq 0$ in $\mathbb{C}[X, Y]$ such that $P(F, G) = 0$.

1.14 Let

$$F = 256\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}, \quad G = 256\frac{(t^2 + t + 1)^3}{t^2(t+1)^2}.$$

Show that $P(F, G) = 0$ for

$$P = X^3Y - 2X^2Y^2 + XY^3 - 1728(X^3 + Y^3) + 1216(X^2Y + XY^2)$$

$$+3538944(X^2 + Y^2) - 2752512XY - 2415919104(X + Y) + 549755813888.$$

(This is related to the simultaneous complex multiplication of two different elliptic curves and also to the André–Oort Conjecture – see Exercise 21.19. Of course the present exercise and the following are illustrations of Littlewood's Principle that "All identities are trivial (once they have been written down by someone else)" as quoted by Cassels.)

1.15 Let

$$F = tu(t^{10} + 11t^5u^5 - u^{10}), \quad G = -t^{20} - u^{20} + 228(t^{15}u^5 - t^5u^{15}) - 494t^{10}u^{10},$$

$$H = t^{30} + u^{30} + 522(t^{25}u^5 - t^5u^{25}) - 10005(t^{20}u^{10} + t^{10}u^{20}).$$

Show that $G^3 + H^2 = 1728F^5$. (This is related to the icosahedron – see Klein, 1956.)

1.16 Let

$$F = 1728\frac{u^3}{u^3 - v^2}, \quad G = -1728\frac{u^2v}{u^3 - v^2}, \quad H = -288\frac{u(tuv - 3u^3 - 4v^2)}{u^3 - v^2},$$

$$K = -24\frac{3t^2u^2v - 18tu^4 - 24tuv^2 + 95u^3v + 16v^3}{u^3 - v^2}.$$

Show that

$$2F^2(F - 1728)^2GK - 3F^2(F - 1728)^2H^2 + (F^2 - 1968F + 2654208)G^4 = 0.$$

(This is related to the differential equation for the modular function – see Exercise 21.15.)

1.17 With $L = 3238$ show that $(t^{1948} + t^{666} + 1)^L (t^{1291} + t^{163} + t)^L$ has a coefficient at least

$$\frac{3^{2L}}{L^2 + L + 1} > 10^{3082}.$$

1.18 Show that there is $P \neq 0$ in $\mathbb{Q}[X]$ for Exercise 1.1.

1.19 Show that there is $P \neq 0$ in $\mathbb{Z}[X]$ for Exercise 1.1.

1.20 Show that there is $P \neq 0$ in $\mathbb{Z}[X, Y]$ for Exercise 1.10.

1.21 Find $P \neq 0$ in $\mathbb{Z}[X, Y]$ with $P(t + i, t - i) = 0$.

1.22 If x, y are in $\mathbb{C}$ with (1.3), must there exist t in $\mathbb{C}$ with (1.2)?

1.23 What about Exercise 1.22 with $\mathbb{C}$ replaced by $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{F}_p$?

2

Irrationality I

The main application of the method of auxiliary polynomials is in diophantine approximation and transcendence. But before these topics comes irrationality: one seeks to prove that a given number is not in $\mathbb{Q}$. One of the earliest examples is of course

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \cdots .$$

It is proved in any elementary text on number theory that e is irrational; the proof is based on the rapid convergence of the series together with the reasonable behaviour of the denominators. We give a proof nevertheless.

Consider the truncation

$$f_n = e - \sum_{k=0}^{n} \frac{1}{k!} = \sum_{k=n+1}^{\infty} \frac{1}{k!}$$

for $n = 0, 1, 2, \ldots$. The first term on the extreme right-hand side dominates and indeed

$$\sum_{k=n+1}^{\infty} \frac{1}{k!} = \frac{1}{(n+1)!} \left(1 + \frac{1}{n+2} + \cdots \right) < \frac{2}{(n+1)!}.$$

Thus $0 < f_n < 2/(n+1)!$ and

$$0 < |n! f_n| < \frac{2}{n+1}. \tag{2.1}$$

Now if s is a denominator for the rational e, then multiplying by s and making n tend to infinity gives a contradiction to the so-called Fundamental Theorem of Transcendence that every non-zero integer has absolute value at least 1.

The proof is slightly easier for the alternating series

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = 1 - 1 + \frac{1}{2} - \frac{1}{6} + \cdots,$$

because we no longer need the dominance.

The proofs extend to give the linear independence over $\mathbb{Q}$ of $1, e, e^{-1}$, which amounts to the fact that e cannot be quadratic over $\mathbb{Q}$. In particular e^2 is irrational. But there is a minor snag. We assume that $r + se + te^{-1} = 0$ for integers r, s, t not all zero, and then for

$$f_n = r + s\sum_{k=0}^{n} \frac{1}{k!} + t\sum_{k=0}^{n} \frac{(-1)^k}{k!} = -s\sum_{k=n+1}^{\infty} \frac{1}{k!} - t\sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!},$$

we get

$$|n!f_n| \le |s|\frac{2}{n+1} + |t|\frac{2}{n+1}.$$

Hence the $n!f_n$ are integers tending to zero as n tends to infinity. But we no longer know that these integers are non-zero as in (2.1).

In fact it is not too hard to show that

$$f_n = f_{n+1} = f_{n+2} = 0 \tag{2.2}$$

is impossible for any n. Namely,

$$(n+1)!(f_{n+1} - f_n) = s + (-1)^{n+1}t$$

and so

$$(n+2)!(f_{n+2} - f_{n+1}) = s - (-1)^{n+1}t.$$

Thus (2.2) would imply $s = t = 0$ so $r = 0$ too, a contradiction.

Here the problem makes its first appearance but is relatively harmless; however in later chapters we will see it getting more and more dangerous.

But as soon as we consider $e^2 = \sum_{k=0}^{\infty} 2^k/k!$ directly, some other difficulties arise. The convergence is practically just as fast, but after truncating at $k = n$ and multiplying by a denominator $n!$, we get a term $2^{n+1}/(n+1)$ which no longer tends to zero.

The proof can be fixed by calculating the power of 2 dividing $n!$ to yield a smaller denominator; this involves restricting n to a special form like 2^m. Such a trick can be extended to give the linear independence over $\mathbb{Q}$ of $1, e^2, e^{-2}$ (see Exercise 2.13); in particular e^4 is irrational. But it is amusing (I learnt it

from the wonderful book of Conway and Guy (1996), p. 253) that these ideas also give the irrationality of $\lambda = e^{\sqrt{2}}$ via

$$\lambda + \frac{1}{\lambda} = 2\sum_{l=0}^{\infty} \frac{2^l}{(2l)!}$$

(see Exercise 2.4).

Actually I know of no such simple proof that e^3 is irrational, although this is not difficult to establish by considering $\int_0^1 e^{3t} t^n (1-t)^n \mathrm{d}t$ (see Exercise 2.14). It can also be done with auxiliary polynomials of the type mentioned in Chapter 1, most efficiently by introducing derivatives as in the differential equation $(e^z)' = e^z$. However some extra arithmetic and analytic machinery is needed. This will be introduced step by step in the following chapters. By these means we will show in Chapter 13 that

$$e^\alpha = \sum_{k=0}^{\infty} \frac{\alpha^k}{k!}$$

is irrational and even transcendental for any rational and even algebraic $\alpha \neq 0$.

In the present chapter we will consider the series

$$\sum_{k=0}^{\infty} \frac{z^k}{2^{k(k-1)/2}} = 1 + z + \frac{1}{2}z^2 + \frac{1}{8}z^3 + \frac{1}{64}z^4 + \cdots, \tag{2.3}$$

which similarly converges for all real and even complex z to a function $f(z)$. It converges faster than the series of e^z, so let us see what truncation of $f(\alpha)$ gives.

Let us start with $\alpha = a/b$, for simplicity taking $a \geq 1, b \geq 1$ in $\mathbb{Z}$. The truncations are

$$f_n = f(\alpha) - \sum_{k=0}^{n} \frac{\alpha^k}{2^{k(k-1)/2}} = \sum_{k=n+1}^{\infty} \frac{\alpha^k}{2^{k(k-1)/2}}.$$

Again there is domination on the extreme right, and if n is large enough we get

$$|f_n| \leq 2\frac{\alpha^{n+1}}{2^{n(n+1)/2}} = \frac{2a^{n+1}}{2^{n(n+1)/2} b^{n+1}}. \tag{2.4}$$

Taking into account a common denominator $2^{n(n-1)/2} b^n$, we deduce

$$|2^{n(n-1)/2} b^n f_n| \leq \frac{2a^{n+1}}{2^n b} = \frac{2a}{b}\left(\frac{a}{2}\right)^n.$$

The proof works if the estimate tends to zero as n tends to infinity (assuming we can rule out the snag $f_n = 0$ as in (2.2) above). Unfortunately this is the case only for $a = 1$.

So all we get by these means is the irrationality of the $f(1/b)$.

In fact we can scrape by with $a = 2$ by estimating the denominators more carefully as with e^2, thanks to the numerators. But we get stuck at $a = 3$, for example, with the irrationality of

$$f(3) = 13.401244574556308427693105053675595778707177552368\ldots$$

For the value $\zeta(3)$ of the Riemann zeta function one had help from Apéry. Instead of his original proof one can consult Beukers's version (Beukers, 1979) – see also Exercise 2.22 – and also the account in van der Poorten (1979). Here an extra ingredient enables us to prove the irrationality of $f(\alpha)$ for all rational $\alpha \neq 0$ using an auxiliary polynomial; and that with only a modicum of extra machinery. Since

$$\frac{(2z)^k}{2^{k(k-1)/2}} = 2z\frac{z^{k-1}}{2^{(k-1)(k-2)/2}},$$

we have the functional equation

$$f(2z) = 1 + 2zf(z) \tag{2.5}$$

and this provides a substitute for the differential equation of e^z.

Namely after replacing z by $z/2$ we get $f(z) = 1 + zf(z/2)$, and we can iterate this to give

$$f(z) = 1 + zf\left(\frac{z}{2}\right) = 1 + z\left(1 + \frac{z}{2}f\left(\frac{z}{4}\right)\right) = \cdots$$

until

$$f(z) = 1 + z + \frac{1}{2}z^2 + \cdots + \frac{1}{2^{(n-1)(n-2)/2}}z^{n-1} + \frac{z^n}{2^{n(n-1)/2}}f\left(\frac{z}{2^n}\right). \tag{2.6}$$

Thus the truncation $f(z) - \sum_{k=0}^{n} z^k/2^{k(k-1)/2}$ is none other than

$$\frac{z^n}{2^{n(n-1)/2}}\left(f\left(\frac{z}{2^n}\right) - 1\right). \tag{2.7}$$

This involves the function $\phi_0(z) = f(z) - 1 = z + \cdots$ (if we take the liberty to change z for a moment). This visibly has a zero of order 1 at $z = 0$, and so for all sufficiently small z we have say

$$|f(z) - 1| \leq 2|z|. \tag{2.8}$$

If we now estimate the truncation f_n at $z = a/b$ using (2.7) and (2.8) (with z changed back again – sorry), then we get exactly the same estimate (2.4) as before. So what if anything has been achieved?

Well, suppose we could find a function $\phi(z)$ instead of $f(z) - 1$ above which has an order of vanishing greater than 1 at $z = 0$. Then we could think about