An Outline of the Thue-Siegel Theorem

Ernie Croot

May 22, 2007

1 Introduction

The Thue-Siegel theorem states that if α is an algebraic number of degree $d \geq 2$, then for every $\varepsilon > 0$ there can be at most finitely many rational numbers

$$\frac{p_1}{q_1},\ \frac{p_2}{q_2},\ \ldots$$

such that

$$\left|\alpha\ -\ \frac{p_i}{q_i}\right|\ <\ \frac{1}{q_i^{2\sqrt{d}+\varepsilon}}. \tag{1}$$

Dyson improved the exponent to $\sqrt{2d} + \varepsilon$, and Roth extended this to the best-possible exponent of $2 + \varepsilon$. All these theorems are ineffective in that they tell you nothing about how large the largest q_i satisfying (1) could be.

The purpose of this paper is to give a somewhat detailed outline of the proof of Siegel's theorem, where we focus more on the ideas rather than certain specific estimates and choices of parameters. One should not think of this note as a good source of quotable facts about Siegel's theorem, because here all the intermediate lemmas we state and prove are vastly weaker and fuzzier than what one would find in, for example, R. Baker's book *Transcendental Number Theory*.

2 An outline

Probably the best outline of the argument that I have seen appears in a paper titled *Determinants in the Study of Thue's Method and Curves with Prescribed Singularities* by Bombieri, Hunt, and van der Poorten. We will

just copy here what they write in that paper, and then in later sections we will expound upon the different steps: First, the method will assume that we have two very good approximations to α, say

$$\left|\alpha - \frac{p_1}{q_1}\right| \ < \ \frac{1}{q_1^{2\sqrt{d}+\varepsilon}}, \text{ and } \left|\alpha - \frac{p_2}{q_2}\right| \ < \ \frac{1}{q_2^{2\sqrt{d}+\varepsilon}}, \tag{2}$$

and we assume that

$$q_1 \ < \ q_2, \text{ and } q_1, q_2 \text{ are very large.}$$

We leave it vague for the time being what we mean by "large"; certainly, if we assume (for proof by contradiction) that there are infinitely many rational approximations to α as good as (2), then there will exist two of them where q_1 and q_2 are as large as we need to make our proof work. The goal will then be to derive a contradiction by following three steps:

Step 1. Construct an auxiliary polynomial $f \in \mathbb{Z}[x, y]$, of bidegree (N_1, N_2) and with small coefficients, such that the initial Taylor coefficients of f at (α, α) vanish.

Step 2. Next, note that $f(p_1/q_1, p_2/q_2)$ is a rational number with denominator at most $q_1^{N_1} q_2^{N_2}$, hence either it is 0 or at least $1/q_1^{N_1} q_2^{N_2}$ in absolute value. Then use the Taylor expansion at (α, α) and step 1 to deduce that (2) implies that $f(p_1/q_1, p_2/q_2)$ is exceedingly small, and so, by the preceeding remark, that $f(p_1/q_1, p_2/q_2) = 0$.

Step 3. Prove directly that, possibly replacing f by a partial derivative of rather small order, we have $f(p_1/q_1, p_2/q_2) \neq 0$, and deduce that we cannot have the two approximations (2), whose existence is supposed in step 2. The basic idea used by Thue, and others, for this step was a two-dimensional version of the obvious fact that a polynomial g in one variable, with rational integral coefficients and with a rational root p/q of multiplicity m, has leading coefficient divisible by q^m, and so would have to be "large". [1]

[1] Despite the fact that the one-dimensional version of this fact about polynomials is "obvious", when one goes to two or more dimensions, the proof becomes much more complicated, and requires a significant new trick. This new trick involves the use of "Wronskian determinants" in two variables, and the fact that they can be factored as $g(x)h(y)$, where $g(x) \in \mathbb{Q}[x]$ and $h(y) \in \mathbb{Q}[y]$.

3 A way to think about the method

One way to think about the proof is that it is a type of "gap principle": Often, one can show that in diophantine equations if there is some solution x or near-solution, then there cannot be any other solution x' that is nearby, in the sense that x' is close to x. One example is rational approximations: Suppose that α is any irrational number and that we have a sequence of rationals $p_1/q_1, p_2/q_2, ...$ (assume they are in lowest terms) such that the ith rational approximates α to within an error of $1/q_i^3$. Then, the q_i's have to get further and further apart (there cannot be infinitely many that are 1 apart, for instance). To see this, note that if $q_1 < q_2$ and we had that

$$\left|\alpha - \frac{p_1}{q_1}\right| \ < \ \frac{1}{q_1^3}, \text{ and } \left|\alpha - \frac{p_2}{q_2}\right| \ < \ \frac{1}{q_2^3},$$

then by the triangle inequality,

$$\left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right| \ \leq \ \frac{1}{q_1^3} + \frac{1}{q_2^3} \ < \ \frac{2}{q_1^3};$$

However, the left-hand-side, being a rational number, has to be at least $1/q_1q_2$, which implies

$$q_1q_2 \ > \ q_1^3/2 \implies q_2 \ > \ q_1^2/2.$$

So, each successive denominator q_{i+1} grows like the square of the previous denominator q_i in the sequence – quite far apart indeed!

Notice that in developing our "gap principle" above we used nothing about the fact that α is algebraic. If we add this assumption, then the rationals p_i/q_i satisfy some extra relations, and we would expect to be able to use these relations to make the gaps even wider. This is one way of thinking of how the proof of the Thue-Siegel works, and in fact it produces a gap so wide that q_1 stays bounded, while q_2 can be forced to be as large as desired. What this means, then, is that there could be no such q_2, and thus there are only finitely many rational approximations p/q to α to within an error $1/q^{2\sqrt{d}+\varepsilon}$.

4 Discussion of the three steps

We make a few stray comments before expounding on Steps 1 through 3 above.

4.1 The choice of N_1 and N_2

We choose both N_1 and N_2 very large, say larger than q_2, such that

$$\frac{1}{q_1^{N_1}} \approx \frac{1}{q_2^{N_2}}$$

To be more precise, we want

$$\frac{1}{q_1^{N_1+1}} < \frac{1}{q_2^{N_2}} \leq \frac{1}{q_1^{N_1}} \tag{3}$$

This can be achieved by picking $N_2 > q_2$ first, and then running through $N_1 = 1, 2, 3, ...$ until the inequality (3) is achieved.

The reason that we want this specific inequality (3) is that in the middle of our calculations we will need to have

$$f(p_1/q_1, p_2/q_2) < 1/q_1^{N_1} q_2^{N_2},$$

but what we will actually show is something like

$$f(p_1/q_1, p_2/q_2) < \max(1/q_1^{2N_1+1}, 1/q_2^{2N_2}).$$

Plainly, the inequality (3) implies that the right-hand-side is smaller than $1/q_1^{N_1} q_2^{N_2}$, as we require.

4.2 The usefulness of dividing by factorials

One of the key requirements in several parts of the proof is that of having the coefficients of certain monomials be integers that are small in absolute value. The coefficients of these monomials are gotten by computing certain mixed partial derivatives. For example, at some point in our proof we start with a monomial $cx^a y^b$; then, we apply the operator $\partial^{i+j}/\partial x^i \partial y^j$, which sends

$$cx^a y^b \quad \rightarrow \quad ca(a-1)\cdots(a-i+1)b(b-1)\cdots(b-j+1)x^{a-i}y^{b-j}.$$

Unfortunately, if i is a small multiple of N_1 or j is a small multiple of N_2, and if the coefficient on the right-hand-side is not 0, then it must be of size at least about $(\kappa N_1)!$ or $(\kappa N_2)!$ in absolute value, for some $\kappa > 0$. But in order for our proofs to work we will need need that this new coefficient is at most $c_0^{N_1+N_2}$, where c_0 depends only on α and not on N_1, N_2, q_1 or q_2.

Fortuntaely, we can divide by $i!j!$ in the above mixed partial calculation, and deduce that

$$\frac{1}{i!j!}\frac{\partial^{i+j}}{\partial x^i \partial y^j}\ cx^a y^b \ = \ c\binom{a}{i}\binom{b}{j}x^{a-i}y^{b-j}.$$

Thus,

- The new coefficient $c\binom{a}{i}\binom{b}{j}$ is an integer if c was an integer; and,

- If the old coefficient c was only of size $c_0^{N_1+N_2}$, where c_0 depends only on α, then this new coefficient is at worst of size $(4c_0)^{N_1+N_2}$, using the trivial upper bounds of 2^{N_1} and 2^{N_2} for these binomial coefficients (since $a \leq N_1$ and $b \leq N_2$).

4.3 Step 1

We suppose that

$$f(x,y) \ = \ \sum_{\substack{0 \leq i \leq N_1 \\ 0 \leq j \leq N_2}} c_{i,j} x^i y^j,$$

where the $c_{i,j}$ are integers yet to be determined. If we expand f at the point (α, α), we have, by the multi-dimensional Taylor theorem, that

$$f(x,y) \ = \ \sum_{\substack{0 \leq i \leq N_1 \\ 0 \leq j \leq N_2}} d_{i,j} (x-\alpha)^i (y-\alpha)^j,$$

where

$$d_{i,j} \ = \ \frac{1}{i!j!}\ \frac{\partial f(x,y)}{\partial x^i \partial y^j}\bigg|_{(x,y)=(\alpha,\alpha)}$$

One can easily see that these $d_{i,j}$ are integer linear combinations of powers of α; and, from the comments in subsection 4.2, one can see that the coefficients in these linear combinations are of size at most

$$B \ := \ 2^{N_1+N_2} \max_{i,j} |c_{i,j}|,$$

and where the powers of α go all the way up to at most $\alpha^{N_1+N_2}$.

What we now want to do is reduce the exponents of these powers of α that occur in the $d_{i,j}$, by using the minimal polynomial of α, to make them

$\leq d-1$. The new coefficients will be rational numbers, but it turns out that we can get good control of the denominators that appear, and we will be able to give nice bounds for the numerators.

We start by assuming that the minimal polynomial of α is given by

$$a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0, \text{ where } a_i \in \mathbb{Z}, \ \gcd(a_0, ..., a_d) \ = \ 1.$$

Now, we have

$$\alpha^d \ = \ \frac{-a_{d-1}\alpha^{d-1} - \cdots - a_0}{a_d}.$$

Multiplying by α, and reusing this relation, we find that

$$\alpha^{d+1} \ = \ \frac{-a_{d-1}\alpha^d - \cdots - a_0\alpha}{a_d} \ = \ \frac{a_{d-1}^2\alpha^{d-1}}{a_d^2} + \cdots$$

And, expanding inductively, we can prove that

$$\alpha^i \ = \ b_{i,d-1}\alpha^{d-1} + \cdots + b_{i,0},$$

where we may write

$$b_{i,\ell} \ = \ \frac{n_{i,\ell}}{a_d^i}, \ n_{i,\ell} \in \mathbb{Z}.$$

(In fact, we can take the denominator to be a_d^{i-d+1} for $j \geq d-1$, but what we have is good enough); furthermore,

$$|n_{i,j}| \ \leq \ c_1^{N_1+N_2},$$

where c_1 depends only on the minimal polynomial of α.

By applying this reduction on the powers of α to each of the coefficients $d_{i,j}$ above, we may write

$$d_{i,j} \ = \ \sum_{k=0}^{d-1} d_{i,j,k}\alpha^k,$$

where

$$d_{i,j,k} \ = \ \frac{n_{i,j,k}}{a_d^{N_1+N_2}},$$

where the $n_{i,j,k}$ are each linear combinations in the undetermined coefficients $c_{u,v}$ of $f(x,y)$ (when expanded about $(0,0)$), and the coefficients in each of these linear combinations of the $c_{u,v}$ is of size at most

$$c_2^{N_1+N_2}, \text{ where } c_2 = c_2(\alpha) \tag{4}$$

depends only on the coefficients of the minimal polynomial of α.

What we want to do now is get all the

$$d_{i,j} \;=\; 0, \text{ whenever } (i,j) \;\leq\; (tN_1, tN_2)$$

(this means $i \leq tN_1$ and $j \leq tN_2$), where we take t as large as possible, while keeping the $c_{u,v}$ bounded by $c_3^{N_1+N_2}$, where $c_3 = c_3(\alpha, \varepsilon)$ depends only on the minimal polynomial of α and on ε.

4.3.1 How big could we possibly take t to be?

Let us not worry about the requirement that $|c_{u,v}| \leq c_3^{N_1+N_2}$, and just consider the largest we could possibly take t to be. Well, in total, $f(x,y)$ has

$$(N_1+1)(N_2+1) \;\sim\; N_1N_2$$

free coefficients $c_{u,v}$. And, for each

$$(i,j) \;\leq\; (tN_1, tN_2),$$

in order to $d_{i,j} = 0$, we need each of the

$$d_{i,j,k} \;=\; 0, \text{ for } k = 0, ..., d-1;$$

so, we have about $dt^2N_1N_2$ homogenous equations that need to be satisfied. As long as the number of variables exceeds the number of equations, there is a non-trivial solution to our system; that is, there is a solution so long as

$$dt^2N_1N_2 \;\lesssim\; N_1N_2.$$

Thus,

$$t \;\lesssim\; \frac{1}{\sqrt{d}},$$

and therefore we might expect that we could take t near $1/\sqrt{d}$.

4.3.2 Siegel's lemma

If we now add in the requirement that the $c_{u,v}$ in all the linear equations be integers, and that they not be too large, we arrive at Siegel's lemma, which gives a way to find such solutions. This lemma is proved by a simple pigeonhole argument: We start by writing our system of approximately $dt^2N_1N_2$ linear equations in the variables $c_{u,v}$ as the equation

$$Ax \;=\; 0, \tag{5}$$

where A is approximately of size $dt^2N_1N_2 \times N_1N_2$, and x is a column vector of length about N_1N_2 consisting of the $c_{u,v}$. The idea is to initially consider *all* vectors v of the form

$$v \;=\; Ay,\; y = (y_1, ..., y_{(N_1+1)(N_2+1)}),\; |y_i| \leq Y,$$

for some value of Y. This Y is to be chosen so that we can guarantee a collision of the form

$$Ay \;=\; Ay',\; \text{all } |y_i|, |y_i'| \;\leq\; Y.$$

Then, letting $x = y - y'$ we get (5). How big are the coordinates of x ? At most of size $2Y$.

How small can we take Y so that we get such collisions? Well, say that D is the maximum absolute value of the entries of A. Note that this D is the maximum of the coefficients of the $c_{u,v}$ that appear in the equations

$$n_{i,j,k} \;=\; 0,\; \text{for all } (i,j) \leq (tN_1, tN_2),\; 0 \leq k \leq d-1,$$

and we said before in (4) that $D < c_2^{N_1+N_2}$.

Now, each of the $\sim dt^2N_1N_2$ coordinates v_i of v satisfy

$$|v_i| \;\leq\; DY\; |\text{columns of } A| \;\leq\; DY(N_1+1)(N_2+1),$$

and yet there are at least $(2Y)^{N_1N_2}$ choices for the y_i; so, we get a collision, basically when

$$(DY(N_1+1)(N_2+1))^{dt^2N_1N_2} \;<\; (2Y)^{N_1N_2},$$

and this occurs as soon as

$$Y \;>\; (D(N_1+1)(N_2+1))^{dt^2(1-dt^2)^{-1}}.$$

Note that if

$$t \ > \ \frac{1}{\sqrt{d}} - \delta, \text{ for some } \delta > 0,$$

then this lower bound will be satisfied if Y satisfies an inequality of the form

$$Y \ > \ c_4^{N_1+N_2}, \text{ where } c_4 = c_4(\alpha, \delta)$$

depends only on the minimal polynomial for α and on δ.

The upshot of this is: We cannot quite get all the $d_{i,j} = 0$, $(i,j) \leq (tN_1, tN_2)$ if we demand that $t = 1/\sqrt{d}$ exactly; but if we allow it to be a little smaller than $1/\sqrt{d}$, say $1/\sqrt{d} - \delta$, then we *can* get the $d_{i,j}$ to vanish, and can do so while having the

$$c_{u,v} \ < \ c_4^{N_1+N_2}, \text{ where } c_4 \ = \ c_4(\alpha, \delta).$$

Henceforth, we will assume that

$$t \ = \ \frac{1}{\sqrt{d}} - \delta,$$

where $\delta > 0$ is "small" relative to ϵ.

4.4 Step 2

Because of our vanishing of coefficients from step 1, we know that every term in $f(x,y)$, when expanded about (α, α), involves a power of $(x-\alpha)$ that exceeds tN_1 or a power of $(y-\alpha)$ that exceeds tN_2. Say such a monomial is

$$C(x-\alpha)^{n_1}(y-\alpha)^{n_2}, \ |C| \ < \ c_4^{N_1+N_2}.$$

Plugging in p_1/q_1 for x and p_2/q_2 for y we find that, in absolute value, this monomial is at most of size

$$|C| q_1^{-n_1(2\sqrt{d}+\varepsilon)} \ \text{ or } \ |C| q_2^{-n_2(2\sqrt{d}+\varepsilon)}.$$

Let us say we are in the case where $n_1 > tN_1$ (instead of $n_2 > tN_2$). Then, the monomial has size at most

$$|C| q_1^{-N_1(1/\sqrt{d}-\delta)(2\sqrt{d}+\varepsilon)}.$$

For δ small enough in terms of ε, this can be made smaller than

$$q_1^{-2N_1-1},$$

because we are thinking of q_1 as being very large, as large as we need, and if we take $\delta > 0$ small enough, and then q_1 large enough, we can absorb the C into this power of q_1, as we have done. In fact, we can make that term smaller than

$$q_1^{-2N_1-1}/N_1N_2$$

in absolute value, which is a more useful bound for us. If the monomial satisfied $n_2 > tN_2$ instead, then we could show that it (the monomial) is smaller than

$$q_2^{-2N_2}/N_1N_2.$$

These bounds on all of the monomials together imply

$$|f(p_1/q_1, p_2/q_2)| \ < \ \max(q_1^{-2N_1-1}, q_2^{-2N_2}) \ \leq \ q_1^{-N_1}q_2^{-N_2}. \tag{6}$$

The right-most inequality follows from our assumption that

$$\frac{1}{q_1^{N_1+1}} \ < \ \frac{1}{q_2^{N_2}} \ \leq \ \frac{1}{q_1^{N_1}}.$$

However, note that since f has bidegree (N_1, N_2) and has integer coefficients $c_{u,v}$, the $f(p_1/q_1, p_2/q_2)$ must be a rational number with denominator that divides $q_1^{N_1}q_2^{N_2}$. Clearly, then, we must have that

$$\text{either} \ \ f(p_1/q_1, p_2/q_2) \ = \ 0, \ \ \text{or} \ \ |f(p_1/q_1, p_2/q_2)| \ \geq \ q_1^{-N_1}q_2^{-N_2}.$$

In order to avoid contradicting (6) we must have

$$f(p_1/q_1, p_2/q_2) \ = \ 0.$$

4.5 Step 3

Suppose we have $f(p_1/q_1, p_2/q_2) = 0$, and write f out in a Taylor series about $(p_1/q_1, p_2/q_2)$ as follows

$$f(x,y) \;=\; \sum_{\substack{0\le i\le N_1\\ 0\le j\le N_2}} e_{i,j}(x-p_1/q_1)^i(y-p_2/q_2)^j. \tag{7}$$

Note that we are assuming $e_{0,0} = 0$.

Now, we claim that there must be some $e_{i,j}$ which is non-zero, where i and j are both "small", say $i \le \varepsilon' N_1$ and $j \le \varepsilon' N_2$, where $\varepsilon' > 0$ can be taken as small as desired, even in terms of ε, so long as N_1 and N_2 are large enough. If so, then

$$g(x,y) \;=\; \frac{1}{i!j!}\frac{\partial^{i+j} f(x,y)}{\partial x^i \partial y^j}.$$

will not vanish at $(p_1/q_1, p_2/q_2)$, and yet it has all the necessary properties to make the argument in step 2 work (well, you need to be careful about how to choose $\delta > 0$.)

Note that, by reasons explained in subsection 4.2, the coefficients of this new function g are no more than a multiple $c_5^{N_1+N_2}$, $c_5 = c_5(\alpha, \delta)$, as large as the coefficients $c_{u,v}$ of $f(x,y)$.

4.5.1 Why must we have $e_{i,j} \neq 0$ for some small (i,j)?

Why must there exist a relatively small index pair (i,j) where $e_{i,j} \neq 0$? Let us first focus on the one-dimensional analogue: Suppose that $f(x)$ is purely a polynomial in x. Then, if we had that

$$f(x) \;=\; \sum_{0\le i\le N_1} e_i(x-p_1/q_1)^i \;\in\; \mathbb{Z}[x]$$

satisfied $e_i = 0$ for $i \le \varepsilon' N_1$, then it would mean that

$$(x-p_1/q_1)^{[\varepsilon' N_1]+1} \;\Big|\; f(x,y);$$

however, since $f(x) \in \mathbb{Z}[x]$, we must therefore have from Gauss's lemma [2] that

$$(q_1 x - p_1)^{[\varepsilon' N_1]+1} \;\Big|\; f(x),$$

which in particular means that $q_1^{[\varepsilon' N_1]+1}$ divides the leading coefficient of $f(x)$, and therefore we would be forced to conclude that the coefficients of f are quite large; indeed, one of them must be of size at least $q_1^{\varepsilon' N_1}$. But if we know that the coefficients are of size at most $c_5^{N_1+N_2}$, then this forces ε' to be rather small for large enough q_1, N_1, and N_2.

4.5.2 A special case for dimension two

When f is a polynomial of both x and y the basic argument from the previous subsection breaks down. Well, there is one special instance where it actually succeeds: Suppose we knew that

$$f(x,y) \;=\; g(x)h(y), \text{ where } g(x) \in \mathbb{Z}[x] \text{ and } h(y) \in \mathbb{Z}[y].$$

And then suppose we had that

$$e_{i,j} \;=\; 0, \text{ whenever } (i,j) \;\leq\; (\varepsilon' N_1, \varepsilon' N_2), \tag{8}$$

where, recall, the $e_{i,j}$ are as given in (7). [3] Then, if we write out

$$g(x) \;=\; \sum_{0 \leq i \leq N_1} g_i (x - p_1/q_1)^i \;\text{ and }\; h(y) \;=\; \sum_{0 \leq j \leq N_2} h_j (y - p_2/q_2)^j,$$

where the $g_i, h_j \in \mathbb{Q}$, we must have that

$$\text{either } \; g_i = 0 \text{ for all } 0 \leq \mathrm{i} \leq \varepsilon' \mathrm{N}_1; \text{ or, } h_j = 0 \text{ for all } 0 \leq \mathrm{j} \leq \varepsilon' \mathrm{N}_2,$$

for, if both of these are false, then the term of lowest degree in $g(x)h(y)$ has $(i,j) \leq (\varepsilon' N_1, \varepsilon' N_2)$, thereby contradiciting our assumption (8).

[2] Actually, what we are using is a corollary of Gauss's lemma. The corollary we use is that if $g(x) \in \mathbb{Q}[x]$ divides a polynomial $f(x) \in \mathbb{Z}[x]$ when division is done in $\mathbb{Q}[x]$, then if we let n be the smallest positive integer so that $ng(x)$ has integer coefficients (so, n is the lcm of the denominators of the coefficients of $g(x)$), we must have that in $\mathbb{Z}[x]$, the polynomial $ng(x)$ divides $f(x)$.

[3] Also note that my notation $(a,b) \leq (c,d)$ means that both $a \leq c$ and $b \leq d$.

Now, if $g_i = 0$ for all $0 \leq i \leq \varepsilon' N_1$, then we deduce that

$$(q_1 x - p_1)^{[\varepsilon' N_1]+1} \;\Big|\; f(x,y),$$

and we are back in the case we analyzed in subsection 4.5.1; specifically, we will have that at least one of the coefficients of $f(x,y)$ exceeds $q_1^{\varepsilon' N_1}$, which means that

$$q_1^{\varepsilon' N_1} \;<\; c_5^{N_1+N_2},$$

which implies that

$$\varepsilon' \;<\; \frac{(N_1+N_2)\log(c_5)}{N_1 \log(q_1)} \;<\; \frac{2\log(c_5)}{\log(q_1)}.$$

So, the bigger q_1 is, the smaller ε' must be.

We get a similar inequality for when $h_j = 0$ for all $0 \leq j \leq \varepsilon' N_2$, namely that

$$\varepsilon' \;<\; \frac{(N_1+N_2)\log(c_5)}{N_2 \log(q_2)} \;\ll\; \frac{\log(c_5)}{\log(q_1)}.$$

The reason that we get roughly the same inequality as for when $g_i = 0$ for lots of values i is that

$$q_1^{N_1} \;\approx\; q_2^{N_2} \quad\Longrightarrow\quad N_1 \log(q_1) \;\asymp\; N_2 \log(q_2)$$

(In this context, $A \approx B$ means that A and B differ by a factor of size at most q_1.)

4.5.3 The general case for dimension two: Wronskians

Ok, so we don't in general have that $f(x,y)$ factors nicely as $g(x)h(y)$, so what can we do? Well, the idea employed by Thue and Siegel is to construct a new polynomial $W(x,y)$ that *does* factor as $g(x)h(y)$, where the coefficients of this new polynomial $W(x,y)$ can be bounded by $c_6^{N_1 N_2}$, where c_6 depends only on α and ε. Furthermore, if the low order coefficients of $f(x,y)$ when expanded about p_1/q_1 and p_2/q_2, as in (7), are all 0, then it will turn out that a similar thing must be true for $W(x,y)$. Then, we will deduce that ε' must be quite small using exactly the same ideas as in subsection 4.5.2.

Let us now describe how to find this $W(x,y)$: First, we know that there exist polynomials

$$\alpha_1(x),...,\alpha_k(x) \ \in \ \mathbb{Q}[x], \text{ and } \beta_1(y),...,\beta_k(y) \ \in \ \mathbb{Q}[y]$$

such that

$$f(x,y) \ = \ \alpha_1(x)\beta_1(y) + \cdots + \alpha_k(x)\beta_k(y).$$

For example, the usual Taylor expansion of $f(x,y)$ provides such $\alpha_i(x)$'s and $\beta_j(y)$'s; however, we want to pick such a set of α's and β's subject to the constraint that

$$k \ \text{ is } \ \text{minimal.}$$

This minimality requirement will force the $\alpha_i(x)$'s to be independent of each other over $\mathbb{Q}$, and the same is true of the $\beta_j(y)$'s (it is a nice and simple exercise to check this!). Note that

$$k \ \leq \ N_2.$$

Now, it is easy to check that

$$\begin{bmatrix} \alpha_1(x) & \alpha_2(x) & \cdots & \alpha_k(x) \\ \frac{\alpha_1'(x)}{1!} & \frac{\alpha_2'(x)}{1!} & \cdots & \frac{\alpha_k'(x)}{1!} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^{(k-1)}(x)}{(k-1)!} & \frac{\alpha_2^{(k-1)}(x)}{(k-1)!} & \cdots & \frac{\alpha_k^{(k-1)}(x)}{(k-1)!} \end{bmatrix} \cdot \begin{bmatrix} \beta_1(y) & \frac{\beta_1'(y)}{1!} & \cdots & \frac{\beta_1^{(k-1)}(y)}{(k-1)!} \\ \beta_2(y) & \frac{\beta_2'(y)}{1!} & \cdots & \frac{\beta_2^{(k-1)}(y)}{(k-1)!} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_k(y) & \frac{\beta_k'(y)}{1!} & \cdots & \frac{\beta_k^{(k-1)}(y)}{(k-1)!} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{f_{0,0}(x,y)}{0!0!} & \frac{f_{0,1}(x,y)}{0!1!} & \cdots & \frac{f_{0,k-1}(x,y)}{0!(k-1)!} \\ \frac{f_{1,0}(x,y)}{1!0!} & \frac{f_{1,1}(x,y)}{1!1!} & \cdots & \frac{f_{1,k-1}(x,y)}{1!(k-1)!} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{f_{k-1,0}(x,y)}{(k-1)!0!} & \frac{f_{k-1,1}(x,y)}{(k-1)!1!} & \cdots & \frac{f_{k-1,k-1}(x,y)}{(k-1)!(k-1)!} \end{bmatrix},$$

where by $f_{a,b}(x,y)$ I mean $\partial^{a+b}f(x,y)/\partial x^a \partial y^b$.

Interestingly, the minimality of k will force these first two matrices to be non-singular (it takes a little work to see this!). So, if you take determinants of both sides, you will get that

$$g(x)h(y) \ = \ W(x,y).$$

But how big are the coefficients of $W(x,y)$? Well, the coefficients of each individual entry in the matrix of which $W(x,y)$ is the determinant, are all bounded from above by $c_6^{N_1+N_2}$, where $c_6 = c_6(\alpha,\varepsilon,\delta)$; so, using your favorite upper bounds for the size of the determinant of a matrix[4] as a function of the size of its entries, you can easily prove that all the coefficients of $W(x,y)$ are bounded from above by (and using the fact that $k \leq N_2$)

$$k! c_6^{k(N_1+N_2)} \ \leq \ N_2! c_6^{N_2(N_1+N_2)} \ < \ N_2! c_6^{2N_1N_2} \ < \ c_7^{N_1N_2},$$

for N_1 and N_2 sufficiently large, for some $c_7 = c_7(\alpha,\varepsilon,\delta)$.

Now expand $W(x,y)$ into a Taylor series about the point $(p_1/q_1, p_2/q_2)$. What we would like to do is use the fact that

$$e_{i,j} \ = \ 0, \text{ for all } (i,j) \ \leq \ (\varepsilon' N_1, \varepsilon' N_2)$$

to show that every term in this taylor expansion either involves a multiple of a large power of $(x - p_1/q_1)$, or a multiple of a large power of $(y - p_2/q_2)$. If we can show this, then the argument in subsection 4.5.2 can be made to work.

But how do we guarantee that the Taylor expansion of $W(x,y)$ has this special property? Well, this is where we need to assume that

$$q_2 \text{ is much larger than } q_1,$$

so much larger that it implies that

$$N_1 \text{ is much larger than } N_2.$$

Then, since $k \leq N_2$, we would have that k is much smaller than N_1. The reason that this helps us is as follows: Consider the first column of the matrix associated to $W(x,y)$. All entries in this first column are just scalar multiples of $f_{j,0}(x,y)$. None of these partials are taken with respect to y, which implies that all the terms in $f(x,y)$ that involve a multiple of $(y - p_2/q_2)^B$, B large, remain mulitples of $(y - p_2/q_2)^B$ when we take partials. But what happens to those terms that are multiples of $(x - p_1/q_1)^A$, A large ? Well, since we take at most k partial derivatives with respect to x for each of $f_{j,0}(x,y)$, the

[4]Actually, it suffices to the the one which says that if M is an $n \times n$ matrix with entries $M_{i,j}$, then its determinant is the sum over $\sigma \in S_n$ of $(-1)^{\text{sgn}(\sigma)} M_{1,\sigma(1)} \cdots M_{n,\sigma(n)}$.

power A in term term in $f(x,y)$ can drop by at most k for the corresponding term in $f_{j,0}(x,y)$; but, if $A \geq \varepsilon' N_1$, then this new power is at least

$$A - k \ \geq \ \varepsilon' N_1 - N_2.$$

A similar thing happens for the second column, and in fact for the first several columns.

Thus, we have that every term in every entry of the first several columns of the matrix corresponding to $W(x,y)$ either involves a large power of $(x - p_1/q_1)$, or a large power of $(y - p_2/q_2)$. The same must clearly be true of the determinant, on using the standard identity for the determinant which involves summing over a certain products of entries of the matrix (some of which are weighted by -1 factors, depending on the sign of certain permuations). Thus, one can imagine that we could now use the idea in subsection 4.5.2 to finish the proof that some small order partial derivative of $f(x,y)$ must not vanish at $(p_1/q_1, p_2/q_2)$.

To make this last assertion precise we need to introduce the concept of the 'index' of a polynomial, which can be thought of as a special type of weighted degree function for our polynomials, and it will satisfy many of the same properties as the degree function.

4.5.4 The index, and the conclusion of the proof

The index has a much more general definition than we actually need for Siegel's theorem. So, here we only state the version we need: Suppose we expand the polynomial $P(x,y)$ of bidegree (N_1, N_2) into a Taylor series about $(p_1/q_1, p_2/q_2)$. Each term of this expansion looks like $c(x - p_1/q_1)^a (y - p_2/q_2)^b$. Among all these terms, consider the maximum value of the expression

$$\frac{a}{N_1} \ + \ \frac{b}{N_2}.$$

This maximal value is called the index of $P(x,y)$, and is written as

$$\mathrm{ind}(P).$$

It is a fairly simple exercise to verify that for two polynomial P and Q,

$$\mathrm{ind}(PQ) \ = \ \mathrm{ind}(P) + \mathrm{ind}(Q),$$

and that

$$\text{ind}(P+Q) \;\geq\; \min(\text{ind}(P), \text{ind}(Q)).$$

Now, from the comments at the end of subsection 4.5.3, one can show that all the entries in the first column of the matrix corresponding to $W(x,y)$ have index at least

$$\varepsilon' \;-\; \frac{N_2}{N_1}.$$

It is also not hard to show that all the entries in the second column have index at least

$$\min(\varepsilon' - 1/N_2,\; \varepsilon' - N_2/N_1).$$

If N_1 is big enough relative to N_2, then this minimum is

$$\varepsilon' - 1/N_2.$$

For such N_1 and N_2 we will further have that the index of all the elements of the jth column, for $j \geq 2$, is at least

$$\varepsilon' \;-\; (j-1)/N_2. \tag{9}$$

Note that this is only positive so long as

$$j \;\leq\; \varepsilon' N_2 + 1,$$

and since the index is always non-negative, we will use the lower bound of 0 for these later columns.

Using (9) as our lower bound for the index, it is not hard to show that

$$\begin{aligned} \text{ind}(W) \quad &\geq \quad (\varepsilon' - N_2/N_1) \;+\; \sum_{1 \leq i \leq \varepsilon' N_2} (\varepsilon' - i/N_2) \\ &= \quad (\varepsilon' - O(\varepsilon'^2))N_2. \end{aligned}$$

Keeping in mind that the coefficients of $W(x,y)$ are bounded from above by $c_7^{N_1 N_2}$, and the fact that $W(x,y)$ factors as $g(x)h(y)$, we will now show that ε' cannot be too large: First, we deduce that

$$\text{either} \;\; \text{ind}(g) \;\geq\; (\varepsilon'/2 - O(\varepsilon'^2))N_2, \;\; \text{or} \;\; \text{ind}(h) \;\geq\; (\varepsilon'/2 - O(\varepsilon'^2))N_2.$$

Suppose that the former holds. Then, we will have that

$$(q_1 x - p_1)^{(\varepsilon'/2+O(\varepsilon'^2))N_1 N_2} \;\Big|\; g(x) \;\Big|\; W(x,y).$$

But this would force at least one of the coefficients of $W(x,y)$ to be of size at least

$$q_1^{(\varepsilon'+O(\varepsilon'^2))N_1 N_2},$$

and so we will have that

$$\varepsilon' + O(\varepsilon'^2) \;<\; \frac{2\log(c_7)}{\log q_1},$$

which means ε' must be small if q_1 is large.

Next, suppose that the latter holds. Then, we will have

$$(q_2 y - p_2)^{(\varepsilon'/2+O(\varepsilon'^2))N_2^2} \;\Big|\; W(x,y).$$

So, some coefficient of $W(x,y)$ must be at least

$$q_2^{(\varepsilon'/2+O(\varepsilon'^2))N_2^2} \;=\; (q_2^{N_2})^{(\varepsilon'/2+O(\varepsilon'^2))N_2} \;>\; (q_1^{N_1})^{(\varepsilon'/2+O(\varepsilon'^2))N_2}.$$

So, again we will have

$$\varepsilon' + O(\varepsilon'^2) \;<\; \frac{2\log(c_7)}{\log q_1}.$$

So,

$$\varepsilon' \text{ must be tiny,}$$

so long as N_1 is much bigger than N_2, and both q_1 and q_2 are very big.