11 Some Applications

We have seen a few examples of how transcendence results can be used to obtain other results of a number theoretic nature, mostly in the form of homework problems. This section further elaborates on some such uses of transcendence results.

Theorem 29. *Let $\mathcal{P}$ denote a fixed non-empty finite set of primes. Consider the set $\mathcal{S}$ of positive integers n which only have prime divisors from the set $\mathcal{P}$. Suppose the elements of $\mathcal{S}$ are $s_1 = 1, s_2, s_3, \ldots$ written in increasing order. Then*

$$s_{i+1} - s_i > \frac{s_i}{(\log s_i)^{c_1}}$$

for $i > 2$ (so $s_i > 2$) and some constant c_1 depending on $\mathcal{P}$.

Proof. Fix $i > 1$. We suppose as we may that $s_{i+1} \leq 2s_i$. Writing

$$\mathcal{P} = \{p_1, p_2, \ldots, p_r\},$$

we obtain

$$s_i = \prod_{i=1}^{r} p_i^{e_i} \qquad \text{and} \qquad s_{i+1} = \prod_{i=1}^{r} p_i^{f_i}$$

for some non-negative integers $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$. Hence,

$$\frac{s_{i+1}}{s_i} = \prod_{i=1}^{r} p_i^{f_i - e_i}.$$

Applying logarithms, we obtain

$$\log\left(\frac{s_{i+1}}{s_i}\right) = \sum_{i=1}^{r} (f_i - e_i) \log p_i.$$

Let A denote the maximum element of $\mathcal{P}$, and set

$$B = \max\{e_1, \ldots, e_r, f_1, \ldots, f_r\} \ll \log s_i.$$

Applying Theorem 22, we deduce that for some constant $c_2 = c_2(\mathcal{P})$,

$$\sum_{i=1}^{r} (f_i - e_i) \log p_i > \frac{1}{(\log s_i)^{c_2}}.$$

We use that

$$\exp(x) > 1 + x \quad \text{for } 0 < x < 1.$$

Hence, exponentiating, we deduce

$$\frac{s_{i+1}}{s_i} > 1 + \frac{1}{(\log s_i)^{c_2}},$$

from which the theorem follows (taking $c_1 = c_2$). □

There are a few different nice results concerning the equation

$$f(x) = by^m, \tag{18}$$

where $f(x) \in \mathbb{Z}[x]$ and b, m, x, and y are in $\mathbb{Z}$. Here, f and b are considered to be fixed and, depending on the result, m may be fixed as well. Two such results which follow from transcendence methods are as follows.

Theorem 30 (Schinzel & Tijdeman). *Let $f(x) \in \mathbb{Z}[x]$, and suppose that $f(x)$ has at least two distinct roots. Let $b \in \mathbb{Z}$ with $b \neq 0$. Then there is a constant c_3 (depending on b and f) such that if m, x, and y are in $\mathbb{Z}$ with $m \geq 0$, $|y| > 1$, and (18) holding, then*

$$m \leq c_3.$$

Theorem 31 (Baker). *Let m and b be integers with $m \geq 3$. Suppose that*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where $\alpha_1 \neq \alpha_2$ and each of α_1 and α_2 are not in the set $\{\alpha_3, \alpha_4, \ldots, \alpha_n\}$. There is a constant c_4 (depending on m, b, and f) such that if (18) holds, then

$$\max\{|x|, |y|\} \leq c_4.$$

As a partial demonstration of such results, we establish the special case of Theorem 30 in which $f(x)$ has at least two simple rational roots. This special case was first established by Tijdeman. For this special case, we will make use of an improvement of Theorem 22 in the case that the β_j are rational integers.

Theorem 22′ (Baker). *Let $\alpha_1, \ldots, \alpha_r$ be non-zero algebraic numbers with degrees at most d and with heights $A_1, A_2, \ldots, A_r$, respecitively. Let $b_1, \ldots, b_r$ be rational integers with absolute value $\leq B$ where $B \geq 2$. Suppose that*

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_r \log \alpha_r \neq 0.$$

Let

$$\Omega = \prod_{j=1}^{r} \log \max\{A_j, 3\} \quad \textit{and} \quad \Omega' = \prod_{j=1}^{r-1} \log \max\{A_j, 3\}.$$

Then there are absolute positive constants C_1 and C_2 such that

$$|\Lambda| > \exp\big(- (C_1 r d)^{C_2 r} \Omega \log \Omega' \log B \big).$$

Proof of Theorem 30, Special Case. Suppose that $f(x)$ has at least two simple rational roots. If a is the leading coefficient of $f(x)$ and n is the degree of $f(x)$, then there is a monic polynomial $g(x) \in \mathbb{Z}[x]$ for which $g(ax) = a^{n-1} f(x)$. Note that $g(x)$ has at least two simple roots that are integers. We consider $g(x)$, and set $b' = a^{n-1} b$. If (18) has a solution in integers with $m = m'$,

$x = x'$, and $y = y'$, then $g(x) = b'y^m$ has a solution with $m = m'$, $x = ax'$, and $y = y'$. Thus, it suffices to consider $f(x)$ monic with two simple integral roots.

Write

$$f(x) = (x - \alpha)(x - \beta)h(x)$$

where α and β are integers and where $h(\alpha)$ and $h(\beta)$ are non-zero. Suppose that (18) holds with $m = m'$, $x = x'$, and $y = y'$, where $m' \geq 0$ and $|y'| > 1$. Observe that if p is a prime divisor of $x' - \alpha$ that also divides $(x' - \beta)h(x')$, then p divides $(\alpha - \beta)h(\alpha)$. Similarly, if p is a prime divisor of $x' - \beta$ that also divides $(x' - \alpha)h(x')$, then p divides $(\alpha - \beta)h(\beta)$. Since (18) holds with $m = m'$, $x = x'$, and $y = y'$, it follows that each prime p that does not divide

$$D = b(\alpha - \beta)h(\alpha)h(\beta)$$

satisfies $p^{rm}||(x' - \alpha)$ and $p^{sm}||(x' - \beta)$ for some *nonnegative* integers r and s. In other words, there are integers u and v such that

$$x' - \alpha = u^m \prod_{p|D} p^{e_p} \quad \text{and} \quad x' - \beta = v^m \prod_{p|D} p^{f_p}$$

for some choice of nonnegative integers e_p and f_p. Furthermore, we may suppose that $0 \leq e_p < m$ and $0 \leq f_p < m$ for each p. We also may suppose that $|u| \geq |v|$ and do so.

If $|u| = |v| = 1$, then

$$\pm \prod_{p|D} p^{e_p} \pm \prod_{p|D} p^{f_p} = \alpha - \beta.$$

Since $\alpha \neq \beta$, we obtain from Theorem 29 that there are finitely many choices of e_p and f_p and, hence, finitely many choices for such x' as in (18). It follows from the condition $|y'| > 1$ that m is bounded.

Now, suppose that $|u| = |v| = 1$ does not hold. Note that the conditions $b \neq 0$ and $|y'| > 1$ imply that $x' \neq \alpha$ and $x' \neq \beta$. This implies that u and v are non-zero. Then, since $|u| \geq |v|$, we deduce $|u| > 1$. We consider $\log(|(x' - \beta)/(x' - \alpha)|)$. Since $\alpha \neq \beta$, we obtain the non-zero expression

$$\Lambda = m \log(|v|/|u|) + \sum_{p|D} (f_p - e_p) \log p.$$

We apply Theorem 22$'$ with $A_1 = \cdots = A_{r-1} = D$, $A_r = |u|$ and $B = m$. Thus, there is a positive constant c_5 (depending on D) such that

$$|\Lambda| > \exp\big(-c_5 \log|u| \log m\big).$$

We use that $\big|\log|1 + x|\big| < 2|x|$ for $|x| < 1/2$. Hence, for m large, there is a positive constant c_6 such that

$$|\Lambda| = \left|\log\left|\frac{x' - \beta}{x' - \alpha}\right|\right| = \left|\log\left|1 + \frac{\alpha - \beta}{x' - \alpha}\right|\right| < 2\left|\frac{\alpha - \beta}{x' - \alpha}\right| < \frac{c_6}{|u|^m}.$$

Comparing the upper and lower bounds for $|\Lambda|$, we see that m is bounded. $\square$

The next result, due to Tijdeman, comes close to resolving a conjecture of Catalan that 3^2 and 2^3 are the only consecutive powers (with exponents > 1) of natural numbers. It shows that there are only finitely many such consecutive powers.

Theorem 32. *There is an absolute constant c_7 such that if $x^m - y^n = 1$ where m, n, x, and y are integers > 1, then $m < c_7$, $n < c_7$, $x < c_7$, and $y < c_7$.*

Sketch of Proof. We may suppose that the exponents m and n are primes, say p and q. By relabelling, we seek to show that the solutions to

$$x^p - y^q = \varepsilon, \tag{19}$$

where p and q are primes with $p \geq q > 1$ and $\varepsilon \in \{1, -1\}$, are bounded. It is not difficult to see further that any solution requires $p \neq q$ (since $(x^p - y^p)/(x - y)$ must exceed 1). Observe that (19) and $p > q$ implies

$$x < y \quad \text{and} \quad \gcd(x, y) = 1.$$

Using results associated with a fixed value of one of the variables implying finitely many solutions in the other variables (results we do not establish here), we may further suppose that

$$x > c_8, \quad y > c_8, \quad p > c_8, \quad \text{and} \quad q > c_8$$

for an arbitrarily fixed constant c_8 (which we take sufficiently large).

From (19), we obtain

$$x^p = y^q + \varepsilon = (y + \varepsilon)(y^{q-1} - \varepsilon y^{q-2} + \cdots + \varepsilon^{q-1}). \tag{20}$$

Setting

$$d = \gcd(y + \varepsilon, y^{q-1} - \varepsilon y^{q-2} + \cdots + \varepsilon^{q-1}).$$

Then $y \equiv -\varepsilon \pmod{d}$ and $y^{q-1} - \varepsilon y^{q-2} + \cdots + \varepsilon^{q-1} \equiv 0 \pmod{d}$ imply $d|q$. Hence, $d = 1$ or $d = q$. A similar argument gives that if q divides $y + \varepsilon$, then q divides $y^{q-1} - \varepsilon y^{q-2} + \cdots + \varepsilon^{q-1}$ (so that $d = q$). In fact, more can be deduced if q divides $y + \varepsilon$. In this case, write $y = -\varepsilon + qt$ where t is an integer. Then

$$y^j \equiv (-\varepsilon)^j + j(-\varepsilon)^{j-1}qt \pmod{q^2}.$$

Using that $(-\varepsilon)^{q-1} = 1$, we deduce

$$\sum_{j=0}^{q-1} (-\varepsilon)^{q-1-j} y^j \equiv \sum_{j=0}^{q-1} (-\varepsilon)^{q-1-j} \big((-\varepsilon)^j + j(-\varepsilon)^{j-1}qt\big) \equiv q + (-\varepsilon)^{q-2}qt \sum_{j=0}^{q-1} j \equiv q \pmod{q^2}.$$

Thus, if q divides $y + \varepsilon$, then q exactly divides $y^{q-1} - \varepsilon y^{q-2} + \cdots + \varepsilon^{q-1}$. By considering the two cases $q \nmid (y + \varepsilon)$ and $q|(y + \varepsilon)$, we deduce from (20) that

$$y + \varepsilon = q^{\delta_1} u^p \qquad \text{where } \delta_1 \in \{-1, 0\}.$$

Similarly,

$$x - \varepsilon = p^{\delta_2} v^q \qquad \text{where } \delta_2 \in \{-1, 0\}.$$

It follows that $u > 1$ and $v > 1$. Using that $q^{\delta_1} u^p = y + \varepsilon > 2$, we obtain

$$q^{\delta_1} u^p - 1 > \frac{q^{\delta_1} u^p}{2} \geq \frac{u^p}{2q}.$$

Therefore,

$$2^p v^{pq} \geq (v^q+1)^p + 1 \geq x^p + 1 \geq y^q \geq (q^{\delta_1} u^p - 1)^q > \left(\frac{u^p}{2q}\right)^q = \frac{u^{pq}}{(2q)^q}.$$

Now, $p > q > c_8$ implies

$$u < 2^{1/q}(2q)^{1/p} v < 2v.$$

Similarly,

$$2^q u^{pq} \geq (u^p+1)^q + 1 \geq y^q + 1 \geq x^p \geq (p^{\delta_2} v^q - 1)^p > \left(\frac{v^q}{2p}\right)^p = \frac{v^{pq}}{(2p)^p},$$

which implies

$$v < 2^{1/p}(2p)^{1/q} u < (4p)^{1/q} u.$$

The above implies that r and s are within a small factor of one another.

From (19), we obtain that

$$(p^{\delta_2} v^q + \varepsilon)^p - (q^{\delta_1} u^p - \varepsilon)^q = \varepsilon.$$

We can rewrite this as

$$\frac{(p^{\delta_2} v^q + \varepsilon)^p}{(q^{\delta_1} u^p - \varepsilon)^q} = 1 + \frac{\varepsilon}{(q^{\delta_1} u^p - \varepsilon)^q}. \tag{21}$$

The idea next is to show q is small compared to p by taking logarithms and applying Theorem 22′. Note that $x = p^{\delta_2} v^q + \varepsilon > c_8$ and $y = q^{\delta_1} u^p - \varepsilon > c_8$, we deduce that $p^{\delta_2} v^q$ and $q^{\delta_1} u^p$ are both large (both $> c_8 - 1$). Since $|\log(1+x)| < 2|x|$ for $0 < |x| < 1/2$, we obtain the following estimates:

$$\left|\log\left(1 + \frac{\varepsilon}{p^{\delta_2} v^q}\right)\right| \leq \frac{2}{p^{\delta_2} v^q} \leq \frac{2p}{v^q}, \tag{22}$$

$$\left|\log\left(1 - \frac{\varepsilon}{q^{\delta_1} u^p}\right)\right| \leq \frac{2}{q^{\delta_1} u^p} \leq \frac{2q}{u^p} \leq \frac{2q}{u^q} \leq \frac{2q}{\left(v/(4p)^{1/q}\right)^q} \leq \frac{8pq}{v^q}, \tag{23}$$

$$\left|\log\left(1 + \frac{\varepsilon}{(q^{\delta_1} u^p - \varepsilon)^q}\right)\right| \leq \frac{2}{(q^{\delta_1} u^p - \varepsilon)^q} \leq \frac{2}{(q^{\delta_1} u^p/2)^q} \leq \frac{2}{q^{\delta_1} u^p/2} \leq \frac{4q}{u^p} \leq \frac{4q}{u^q} \leq \frac{16pq}{v^q}. \tag{24}$$

We set

$$\Lambda = \delta_2 p \log p - \delta_1 q \log q + pq \log(v/u).$$

To apply Theorem 22′, we justify first that $\Lambda \neq 0$. Equivalently, we show $\log\left(p^{\delta_2 p} v^{pq} / q^{\delta_1 q} u^{pq}\right) \neq 0$. This in turn is equivalent to showing

$$(x - \varepsilon)^p - (y + \varepsilon)^q \neq 0.$$

If $\varepsilon = 1$, then

$$(x-\varepsilon)^p - (y+\varepsilon)^q < x^p - (y+1)^q < x^p - y^q - qy^{q-1} = 1 - qy^{q-1} < 0;$$

and if $\varepsilon = -1$, then

$$(x-\varepsilon)^p - (y+\varepsilon)^q > (x+1)^p - y^q < x^p - y^q + px^{p-1} = 1 + px^{p-1} > 0.$$

Thus, $\Lambda \neq 0$.

From (21), we deduce that

$$\Lambda + p\log\left(1 + \frac{\varepsilon}{p^{\delta_2}v^q}\right) - q\log\left(1 - \frac{\varepsilon}{q^{\delta_1}u^p}\right) = \log\left(1 + \frac{\varepsilon}{(q^{\delta_1}u^p - \varepsilon)^q}\right).$$

From (22), (23), and (24), we deduce

$$|\Lambda| \leq \frac{26p^2}{v^q}.$$

We apply Theorem 22$'$ with $\alpha_1 = p$, $\alpha_2 = q$, and $\alpha_3 = v/u$. Note that $\log(pq) \leq 2\log p$. We deduce

$$|\Lambda| > \exp\big(-c_9(\log p)(\log q)(\log v)(\log\log p)(\log p)\big) > \exp\big(-c_9(\log p)^4(\log v)\big)$$

for some constant $c_9 > 0$. Combining these estimates for $|\Lambda|$, we obtain

$$q\log v - 2\log p + O(1) < (\log p)^4(\log v)$$

which easily implies

$$q \ll (\log p)^4. \tag{25}$$

We apply Theorem 22$'$ now to estimate

$$\Lambda' = p\log\big(p^{\delta_2}v^q + \varepsilon\big) - \delta_1 q\log q - pq\log u.$$

We check that

$$\Lambda' = \log\big((p^{\delta_2}v^q + \varepsilon)^p/(q^{\delta_1 q}u^{pq})\big) = \log\big(x^p/(y+\varepsilon)^q\big) \neq 0$$

by considering the cases $\varepsilon = 1$ and $\varepsilon = -1$. For $\varepsilon = 1$, $x^p/(y+\varepsilon)^q \neq 1$ since

$$x^p - (y+1)^q < x^p - y^q - qy^{q-1} < 0.$$

For $\varepsilon = -1$, we use that $(y-1)^q < (y-1)y^{q-1}$ so that $x^p/(y+\varepsilon)^q \neq 1$ since

$$x^p - (y-1)^q > x^p - y^q + y^{q-1} > 0.$$

Next, observe that from (21) we have

$$\Lambda' - q\log\left(1 - \frac{\varepsilon}{q^{\delta_1}u^p}\right) = \log\left(1 + \frac{\varepsilon}{(q^{\delta_1}u^p - \varepsilon)^q}\right).$$

We combine (23) and (24) to obtain

$$|\Lambda'| \leq \frac{6q}{u^p}.$$

Since $u > 1$ and $p > q > c_8$, we deduce

$$-\log|\Lambda'| \geq p\log u - \log(6q) \geq -c_{10}p\log u \tag{26}$$

for some $c_{10} > 0$.

On the other hand, we can write

$$\Lambda' = p \log \left(\frac{p^{\delta_2} v^q + \varepsilon}{u^q} \right) - \delta_1 q \log q.$$

We apply Theorem 22′ with $\alpha_1 = q$ and $\alpha_2 = (p^{\delta_2} v^q + \varepsilon)/u^q$. As $\delta_2 \in \{-1, 0\}$, we deduce from $u < 2v$ that the height of α_2 is bounded by

$$\max\{v^q + p, pu^q\} \leq 2^q p v^q.$$

Set $H = 2^q p v^q$ and note that $v > 1$ implies

$$\log H \ll \log p + q \log v \ll q(\log p)(\log v).$$

We deduce from Theorem 22′ that

$$|\Lambda'| > \exp\big(-c_{11}(\log q)(\log H)(\log\log q)(\log p)\big) > \exp\big(-c_{12} q (\log p)^4 (\log v)\big)$$

for some positive constants c_{11} and c_{12}. From $v < (4p)^{1/q} u$, we have

$$\log v < \log u + \frac{\log(4p)}{q}.$$

Using (25), (26), and $p > q > c_8$, we obtain

$$p \log u < c_{13} (\log p)^8 (\log u)$$

for some $c_{13} > 0$. This inequality implies p is bounded. As $p > q$, we also have that q is bounded. Taking $f(x) = x^p - \varepsilon$, $b = 1$, and $m = q$, we deduce from Theorem 31 that the values of x and y are also bounded. The theorem follows. $\square$