3 Third assignment with solutions

1. Let a be a positive integer > 20. We will solve $1+a^x = (a+1)^y$ in integers $x, y \geq 0$ using the polynomial method given in the proof of the Siegel-Mahler Theorem and show that $x = y = 1$ is the only solution. Assume that we are given a solution x, y and suppose that $x > 1$.

   (a) Show that $x \geq y \geq 0.9x$.

   (b) Show that x is odd.

   (c) Let $x = 2n + 1$. Using Corollary 4.3.5 construct integers A, B, C such that $aA + a^{2n+1}B = a(a+1)^{2n}C$ and $aA \neq B$ and $|A|, |B|, |C| \leq (6\sqrt{3})^n(a+1)^n$.

   (d) Replace in the above equality $a^{2n+1} = a^x$ by $(a+1)^y - 1$ and show that we get a contradiction. (Hint: see proof of Corollary 4.3.6).

   Solution:

   (a) Note that also $y > 1$. We have trivially, $a^x + 1 = (a+1)^y > a^y + 1$. Hence $x > y$. To estimate y from below, write

   $$\begin{aligned} y &= \log(a^x + 1)/\log(a+1) \\ &> x\log(a)/\log(a+1) \end{aligned}$$

   Since $a > 20$ we verify that $\log(a)/\log(a+1) > 0.98 > 0.9$. Hence our lower bound follows.

   (b) Consider the equality modulo $a+1$. We get $(-1)^x + 1 \equiv 0 (\text{mod } a+1)$. Since $a > 1$ this implies that x must be odd.

   (c) Apply Corollary 4.3.5 with $b = 1, c = a+1, \lambda = a$. Let $B = A_n, A = B_n, C = C_n$. Then multiply the equality $a^{2n}B + A = (a+1)^{2n}C$ by a.

   (d) Replace $a^x = a^{2n+1}$ by $(a+1)^y - 1$ to get $aA + (a+1)^y B - B = a(a+1)^{2n}C$. Since $2n \geq y$ we see that $(a+1)^y$ divides $aA - B$. Since $aA - B$ is non-zero by contruction this implies that

   $$(a+1)^y \leq |aA - B| \leq (a+1)(6\sqrt{3})^n(a+1)^n.$$

   We use $y > 0.9x = 1.8n + 0.9$ to get $(a+1)^{1.8n+0.9} \leq (6\sqrt{3})^n(a+1)^{n+1}$. Hence

   $$0.8n - 0.1 \leq \log(6\sqrt{3})/\log(a+1) < 0.8.$$

   The latter inequality follows because $a > 20$. So we conclude that $n \leq 1$. Hence $x = 2n+1 = 3$. So $y < 3$ and we are left with $a^3 + 1 = (a+1)^2$ or $a^3 + 1 = (a+1)$. Both equations are impossible when $a > 20$.

2. Let $f, g \in \mathbb{Z}[x]$ be two polynomials and suppose that g has at least three distinct zeros and f, g have no common zeros. We introduce the concept of resultant in the following two questions.

(a) Suppose that f, g have degrees m, n respectively. Show that there exist non-trivial polynomials $A, B \in \mathbb{Z}[x]$ of degrees at most $n-1, m-1$ and an integer R such that $Af + Bg = R$. (Hint: use (linear) algebra). Note that in a similar way one can prove the existence of non-trivial polynomials $C, D \in \mathbb{Z}[x]$ of degrees at most $n-1, m-1$ and $S \in \mathbb{Z}$ such that $Cf + Dg = Sx^{m+n-1}$.

(b) Let R, S be the integers of the previous question. Show that $R, S \neq 0$ (the smallest possible positive R is called the *resultant* of f and g).

(c) Prove that the number of rational numbers a/b such that $f(a/b)/g(a/b) \in \mathbb{Z}$ is finite. (Hint: Homogenize $f(a/b), g(a/b)$ by multiplication with appropriate powers of b so that they become integers. Then use parts (a) and (b))

Solution:

(a) Let $f = f_m x^m + \cdots + f_1 x + f_0$ and $g = g_n x^n + \cdots + g_1 x + g_0$. We need to find polynomials $A = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $B = b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ such that $R = Af + Bg$ is a constant polynomial. That means the coefficients of R are all zero, except for the constant term. This gives us a set of $m+n-1$ homogeneous linear equations in the $m+n$ unknowns a_i, b_j. So there exists a non-trivial solution in $\mathbb{Q}$. After multiplication with a common denominator we can assume that we have a non-trivial integer solution.

The second part is completely similar, the only difference being that the constant term is now set to zero and the coefficient of x^{m+n-1} is not. So we have again $m+n-1$ homogeneous linear equations.

(b) Suppose that $R = 0$. So $Af + Bg = 0$ and f divides Bg. It is given that f, g are relatively prime, so we get that f divides A. Since the degree of A is less than the degree of f this is only possible if $A = 0$. Hence $B = 0$, contradicting the non-triviality of our solution. So we conclude that $R \neq 0$. Similarly we show that $S \neq 0$.

(c) We use the following convention: if $P(z)$ is a polynomial of degree d, then we write $P(a, b) = b^d P(a/b)$. Suppose $f(a/b)/g(a/b)$ is an integer. Let us suppose f has degree m and g has degree n. Assume first that $n \leq m$. Then $b^{m-n}g(a, b)$ divides $f(a, b)$. Let A, B be as in part (a). Then

$$A(a, b)f(a, b) + B(a, b)g(a, b) = Rb^{m+n-1}.$$

Since $g(a, b)$ divides $f(a, b)$ we deduce that $g(a, b)$ divides Rb^{m+n-1}. Letting C, D be as above we get $C(a, b)f(a, b) + D(a, b)g(a, b) = Sa^{m+n-1}$. So $g(a, b)$ divides Sa^{m+n-1}. Since a, b are relatively prime we conclude that $g(a, b)$ divides $\mathrm{lcm}(R, S)$. So $g(a, b)$ can assume at most finitely many values. The finiteness of the solutions of the Thue equation implies that we have finitely many possible pairs a, b.

The case $n > m$ is a bit harder. We get that $g(a, b)$ divides $b^{n-m}f(a, b)$. From $A(a, b)f(a, b) + B(a, b)g(a, b) = Rb^{n+m-1}$ multiplied by b^{n-m} we conclude that

$g(a,b)$ divides Rb^{2n-1}. We use a variant. Let $\tilde{f} = z^n f(1/z)$ and $\tilde{g} = z^n g(1/z)$. Note that $\tilde{f}$ and $\tilde{g}$ are relatively prime and have degree n. So there are polynomials $\tilde{A}, \tilde{B} \in \mathbb{Z}[z]$ of degree at most $n-1$ such that $\tilde{A}\tilde{f} + \tilde{B}\tilde{g} = \tilde{R} \in \mathbb{Z}$ is non-zero. Now substitute $z = b/a$ and multiply out the denminator a^{2n-1}. Note also that $a^n \tilde{f}(b/a) = b^{n-m} f(a,b)$ and $a^n \tilde{g} = g(a,b)$. We get $\tilde{A}(a,b)b^{n-m} f(a,b) + \tilde{B}(a,b)g(a,b) = \tilde{R}a^{2n-1}$. Hence $g(a,b)$ divides $\tilde{R}a^{2n-1}$ we conclude that $g(a,b)$ divides $\mathrm{lcm}(R, \tilde{R})$ and we draw our finiteness conclusion again.

3. In this exercise you are asked to apply the estimate of Laurent, Mignotte and Nesterenko (see Exercises of 'linear form in logarithm' notes) to more advanced equations.

   (a) Prove that the equation
   $$x^n - 2y^n = 1$$
   in unknowns x, y with $x \geq 2, y \geq 2$ has no solutions if $n > 10000$. (Hint: Applying Laurent-Mignotte-Nesterenko to an appropriate linear form in two logarithms you will get a lower estimate depending on x, y and n. But you can derive also an upper estimate which depends on x, y, n. Comparison of the two estimates leads to an upper bound for n independent of x, y.

   (b) Let a, b, c be positive integers. Prove that there is a number $C > 0$, effectively computable in terms of a, b, c, such that the equation
   $$ax^n - by^n = c$$
   has no solutions in $x, y \geq 2$ if $n > C$. In the case $a = b$ give an elementary proof, without using the result of Laurent-Mignotte-Nesterenko.

   (c) Prove that the equation
   $$y^z = \binom{x}{3}$$
   integers x, y, z with $x > 3, y \geq 2, z \geq 2$ has only finitely many solutions. (Hint: factor the right hand side).

   Solution:

   (a) Let x, y, n be integers with $x \geq 2$, $y \geq 2$, $n \geq 3$ and $x^n - 2y^n = 1$. Then $|1 - 2(y/x)^n| = 1/x^n$ and in view of the inequality $|\log(1+x)| \leq 2|x|$ for $x \in \mathbb{R}$ with $|x| \leq 1/2$,
   $$\Lambda := |\log 2 + n \log(y/x)| \leq 2e^{-n \log x}.$$
   On the other hand, by Laurent-Mignotte-Nesterenko, using $x \geq y \geq 2$,
   $$\begin{aligned} \log \Lambda &\geq -22 \left(\max \left\{ \log \left(\frac{1}{\log x} + \frac{n}{\log 2} \right) + 0.06,\ 21 \right\} \right)^2 \log 2 \log x \\ &\geq -22 \left(\max \left\{ \log \left(\frac{n+1}{\log 2} \right) + 0.06,\ 21 \right\} \right)^2 \log 2 \log x \\ &\geq -22 \left(\max\{\log(n+1) + 0.43,\ 21\} \right)^2 \log 2 \log x. \end{aligned}$$

Combined with the upper bound for Λ established above, this yields

$$n \log x - \log 2 \leq 22 \left(\max\{\log(n+1) + 0.43,\, 21\}\right)^2 \log 2 \log x.$$

We can now divide by $\log x$ and obtain

$$n \leq 22 \left(\max\{\log(n+1) + 0.43,\, 21\}\right)^2 \log 2 + 1.$$

In case the maximum is 21, we get $n \leq 22 \times 21^2 \log 2 + 1 < 6726$. In case the maximum is $\log(n+1)+0.43$ we get an inequality which is impossible for $n > 1000$.

(b) First assume that $a \neq b$. Let x, y, n be integers with $x \geq 2, y \geq 2, n \geq 3$ and $ax^n - by^n = c$. In case that $x = y$ we have $2^n \leq x^n = c/(a-b)$ and we are done. Assume also that $x \neq y$. Assume for instance that $x > y$, otherwise interchange a, x and b, y and replace c by $-c$. Then arguing as in a), we see that on the one hand,

$$\Lambda := |\log(b/a) + n \log(y/x)| \leq 2|1 - (b/a)(y/x)^n| \leq |2c/a| \cdot e^{-n \log x},$$

on the other hand, by Laurent-Mignotte-Nesterenko, assuming that n is so large that in the maximum 21 is the smallest,

$$\log \Lambda \geq -\gamma_1 (\log n)^2 \log x$$

for some effectively computable number γ_1 depending on a, b, c. Comparing the upper and lower bound for $\log \Lambda$ we can divide out $\log x$, and derive $n \leq \gamma_2 (\log n)^2$ for some constant γ_2. This implies that n is bounded.

Now assume that $a = b$. Then by dividing by a we get an equation $x^n - y^n = c'$, say. Assume for instance that $c' > 0$. Let (x, y) be a solution. Then necessarily, $x > y \geq 2$, and so,

$$n 2^{n-1} \leq n(x-1)^{n-1} \leq x^n - (x-1)^n \leq x^n - y^n = c'.$$

Hence n is bounded.

(c) For a prime p and an integer m we write $pk \| m$ if p^k divides m but p^{k+1} does not divide m.

We rewrite the equation as

$$6y^z = x(x-1)(x-2).$$

In case that $z = 2$ we have a (hyper)elliptic equation which has only finitely many solutions x, y. Take a solution x, y, z with $y \geq 2$, $z \geq 3$, $x \geq 3$. We want to split off as large as possible z-th powers from $x, x-1, x-2$ and to this end we investigate for each prime p with which power it divides $x, x-1, x-2$.

First let $p = 2$. Assume that $2^a \| x$, $2^b \| x-1$, $2^c \| x-2$. If x is odd, then $a = c = 0$ and $b \equiv 1 \pmod{z}$. If x is even, then $b = 0$ and one of a, c is 1 since x, $x-2$

cannot both be divisible by 4. So either $a = 1$ and $c \equiv 0 \pmod{z}$, or $c = 1$ and $a \equiv 0 \pmod{z}$.

Next let $p = 3$. Precisely one of $x, x-1, x-2$ is divisible by 3, and this must then be with exponent $\equiv 1 \pmod{z}$. Finally, let p be a prime larger then 3. Then p divides at most one of $x, x-1, x-2$, and this must then be with exponent $\equiv 0 \pmod{z}$. It follows that $x = \alpha u^z$, $x - 1 = \beta v^z$, $x - 2 = \gamma w^z$, where $\alpha, \beta, \gamma \in \{1, 2, 3, 6\}$ and u, v, w are positive integers.

Assuming $x \geq 8$ as we may, we have $u, v, w \geq 2$. Hence $\alpha u^z - \beta v^z = 1$ with $u, v \geq 2$ and $z \geq 3$ and with $\alpha, \beta \in \{1, 2, 3, 6\}$. By b) there is an effectively computable constant C such that $z < C$. For fixed $z \geq 3$, α, β this equation has by Thue's theorem only finitely many solutions u, v and this leads to only finitely many possibilities for x. So altogether, $y^z = \binom{x}{3}$ has only finitely many solutions.