Exercises on linear forms in the logarithms of algebraic numbers

Yann Bugeaud

Exercise 1.
Prove that the equation
\[ y^2 + 1 = x^m \]
has no solutions in rational integers (V. A. Lebesgue, 1850).

Exercise 2.
Prove that the Diophantine equation
\[ x^2 + 7 = 2^n \]
has exactly five integer solutions, given by
\[ (x, n) \in \{(1, 3), (3, 4), (5, 5), (11, 7), (181, 15)\}. \]

Hint. Prove that \( n = 4 \) gives the only solution with \( n \) even. Assume that \( n \) is odd and write \( n = 2m + 1, y = 2^m \). Consider the equation
\[ x^2 - 2y^2 = -7. \]
Prove that \( y \) is an element of the binary recurrence sequence \((y_s)_{s \in \mathbb{Z}}\) defined by
\[ y_0 = 2, \quad y_1 = 3 \quad \text{and} \quad y_{s+2} = 2y_{s+1} + y_s, \quad s \in \mathbb{Z}. \]
We aim to show that the only elements of \((y_s)_{s \in \mathbb{Z}}\) which are powers of 2 are \( y_{-6} = 128 \) and \( y_0 = 2 \). Show that we can restrict ourselves to study the sequence \((u_s)_{s \in \mathbb{Z}}\), given by
\[ u_s = y_{8s-6}/8, \text{ that is, by the binary recurrence} \]
\[ u_0 = 16, \quad u_1 = 1 \quad \text{and} \quad u_{s+2} = 1154u_{s+1} - u_s. \]
Prove that if \( y = 2^m \) for some \( m \geq 8 \), then \( y = 8u_s \) for some \( s \equiv 16 \mod 32 \).
Look at the sequence \((u_s)_{s \in \mathbb{Z}}\) modulo the prime number 7681. Use the quadratic reciprocity law to show that, for any \( s \equiv 16 \mod 32 \), the number \( u_s \) cannot be a power of 2. Conclude.

Exercise 3.
Let \( \alpha_1, \ldots, \alpha_n \) be algebraic numbers. Let \( b_1, \ldots, b_n \) be non-zero integers. Deduce from Theorem A a lower bound for the quantity
\[ \Lambda := |\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1|, \]
when \( \Lambda \neq 0 \). (Consider separately the case where all the \( \alpha_i \) are real.)
Exercise 4.
Let $d$ be a non-zero integer and consider the Diophantine equation
\[ x^2 + d = y^p, \quad \text{in } x > 0, \ y > 0 \text{ and } p \geq 3 \text{ prime}. \]
Use Theorem A to get an upper bound for $p$ when $d = -2, \ d = 2, \ d = 7, \text{ and } d = 25,$ respectively.

Exercise 5.
Let $f(X)$ be an irreducible integer polynomial of degree at least 3. Prove that the equation
\[ f(x) = y^2 \]
has only finitely many integer solutions $x, y$.

Exercise 6.
Consider the Diophantine equation
\[ x^2 + a^2 = 2y^p, \]
where $a$ is a given positive integer, $x, y$ are coprime integers, and $p > 3$ is a prime.
Show that there exists an absolute constant $C$ such that $p \leq C \log(2a)$.

Exercise 7.
Let $a, b, k$ be non-zero integers. Prove that the equation
\[ ax^m - by^n = k, \]
in the four unknowns $x \geq 2, \ y \geq 2, \ m \geq 3, \ n \geq 2,$ has only finitely many solutions if one of the unknowns is fixed.

Exercise 8.
Consider the Diophantine equation in four unknowns
\[ \frac{x^n - 1}{x - 1} = y^q. \]
Prove that it has only finitely many solutions if $x$ is fixed or if $n$ has a fixed prime divisor or if $y$ has a fixed prime divisor.
Assume that $x$ is a perfect square, $x = z^2$. Establish then an absolute (i.e., independent of $x$) upper bound for $q$. 

2
Exercise 9.

Let $\xi$ be an irrational, real, algebraic number. Let $\left(\frac{p_n}{q_n}\right)_{n \geq 1}$ be the sequence of convergents to $\xi$. Use Baker’s theory to get an effective lower bound for $P[p_nq_n]$, where $P[\cdot]$ denotes the greatest prime factor.

*Open problem:* To get an effective lower bound for $P[p_n]$ (resp. for $P[q_n]$).

Exercise 10.

Give an explicit lower bound for the greatest prime factor of $k(k-1)$, when the integer $k$ goes to infinity.

Exercise 11.

Using only elementary method, show that there exists an absolute constant $C$ such that

$$v_5(3^m - 1) \leq C \log m, \quad \text{for any } m \geq 2.$$ 

More generally, let $K$ be a number field of degree $d$, let $p$ be a prime number and $\mathcal{P}$ be a prime ideal in $O_K$ dividing $p$. Then, for any algebraic integer $\alpha$ in $K$ and any positive integer $m \geq 2$ such that $\alpha^m \neq 1$, there exists a positive constant $C$, depending only on $d$, $p$ and $\alpha$, such that

$$v_{\mathcal{P}}(\alpha^m - 1) \leq C \log m.$$ 

Exercise 12.

Let $p_1, \ldots, p_\ell$ be distinct prime numbers. Let $S$ be the set of all positive integers of the form $p_1^{a_1} \cdots p_\ell^{a_\ell}$ with $a_i \geq 0$. Let $1 = n_1 < n_2 < \ldots$ be the sequence of integers from $S$ ranged in increasing order. As above, let $P[\cdot]$ denote the greatest prime divisor. Give an effective lower bound for $P[n_{i+1} - n_i]$ as a function on $n_i$.

Exercise 13.

Let $a$, $b$, $c$ and $d$ be non-zero integers. Let $p$ and $q$ be coprime integers. Prove that the Diophantine equation

$$ap^x + bq^y + cp^z + dq^w = 0,$$

in non-negative integers $x, y, z, w$, has only finitely many solutions.

Exercise 14.

Let $\alpha > 1$ and $d > 1$ be an integer. Suppose that $(x, y, m, n)$ with $y > x$ is a solution of the Diophantine equation

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}.$$ 

Assume that

$$\gcd(m - 1, n - 1) = d, \quad \frac{m - 1}{n - 1} \leq \alpha.$$ 

Apply Baker’s theory to bound $d$ by a linear function of $\alpha$. 

3
Exercise 15.

Consider the Diophantine equation \( x^2 - 2^m = y^n \) in positive integers \( y > 1, n > 2, x, m \), with \( x \) and \( y \) coprime. Show that \( n \) is bounded by an absolute numerical constant. What happens if 2 is replaced by an odd prime number \( p \)?

Exercise 16.

Let \( P \geq 2 \) be an integer and \( S \) be the set of all integers which are composed of primes less than or equal to \( P \). Show that there are only finitely many quintuples \((x, y, z, m, n)\) satisfying
\[
x^m - y^n = z^{\langle m,n \rangle},
\]
with \( x, y, m, n \) all \( \geq 2 \) and \( z \) in \( S \), where \( \langle m, n \rangle \) denotes the least common multiple of \( m \) and \( n \).

Exercise 17.

Consider the Diophantine equation
\[
2^a + 2^b + 1 = y^q,
\]
in integers \( a > b > 0, q \geq 2, y \geq 2 \). Prove that \( q \) is bounded.

Consider the Diophantine equation
\[
2^a + 2^b + 2^c + 1 = y^q,
\]
in integers \( a > b > c > 0, q \geq 2, y \geq 2 \). Prove that \( q \) is bounded.

What happens if one replaces 2 in the above equations by an odd prime number \( p \)?

Exercise 18.

Let \( a \geq 1, b, c \) be non-zero integers. Prove that the equation
\[
ax^n - by^n = c,
\]
in the unknowns \( x \geq 2, y \geq 2, n \geq 3 \) has only finitely many solutions.

Show that if \( c \) and \( a - b \) are very small compared to \( a \), then one gets an upper bound for \( n \) independent of \( a, b, c \).

Exercise 19.

Deduce Theorem F from Theorem C.

**Hint.** Establish first that, for integers \( b_1, \ldots, b_n \) and \( N \geq Q \geq 1 \), there exist a positive integer \( r \) and integers \( p_1, \ldots, p_n \) such that \( \lfloor N/Q \rfloor \leq r \leq N \) and
\[
|b_i - rp_i| \leq rQ^{-1/n} + |b_i|/(2r - 1) \quad (i = 1, \ldots, n).
\]
Then, consider the algebraic numbers \( \alpha = \alpha_1^{p_1} \cdots \alpha_n^{p_n} \) and \( \gamma = \alpha_1^{b_1-rp_1} \cdots \alpha_n^{b_n-rp_n} \alpha_{n+1} \).