An $ax + by + cz = 0$ conjecture

Conjecture. We are given positive integers a, b, c, pairwise coprime and satisying $a \leq b+c$, $b \leq c+a$ and $c \leq a+b$. Then there exists a finite number, n say, of integer solutions $(x_i, y_i, z_i) \neq (0,0,0)$ $(i = 1, \ldots, n)$ of $ax + by + cz = 0$ such that

$$\{x_1, \ldots, x_n\} = \{y_1, \ldots, y_n\} = \{z_1, \ldots, z_n\}, \qquad (*)$$

as multisets.

Lemma. Assuming (as wlg we can) that $\gcd(a, b, c) = 1$ then each of the conditions on a, b, c in the conjecture is necessary.

Proof. Suppose that $a > b + c$ and, wlg, that x_1 has maximal modulus among all the x_i's. Then, by (*), also $|y_1| \leq |x_1|$ and $|z_1| \leq |x_1|$. Note that $x_1 \neq 0$. Hence

$$a|x_1| = |-ax_1| = |by_1 + cz_1| \leq (b + c)|x_1|,$$

so that $a \leq b + c$. Similarly $b \leq c + a$ and $c \leq a + b$.

Now take a prime p, and among the x_i assume wlg that x_1 is divisible by the smallest power of p (i.e., it has maximal p-adic valuation). Then, by (*), $|y_1|_p \leq |x_1|_p$ and $|z_1|_p \leq |x_1|_p$. Hence $|ax_1| = |-by_1 - cz_1|_p \leq \max(|b|_p, |c|_p)|x_1|_p$ and so, since $x_1 \neq 0$, $|a|_p \leq \max(|b|_p, |c|_p)$. Since $\gcd(a, b, c) = 1$, b and c cannot both be divisible by p. Doing this for all primes p, we have $\gcd(b, c) = 1$. Similarly $\gcd(c, a) = \gcd(a, b) = 1$.

Applications.

Theorem. Suppose the conjecture holds. Then the equation $ax + by + cz = 0$ has a solution in nonzero conjugate algebraic integers iff a, b and c satisfy the conditions in the conjecture.

Proof. Suppose that α_1, α_2 and α_3 are, conjugate, nonzero, and that $a\alpha_1 + b\alpha_2 + c\alpha_3 = 0$. Let N be a normal extension of $\mathbb{Q}$ containing α_1 By applying to $a\alpha_1 + b\alpha_2 + c\alpha_3 = 0$ an automorphism of N that takes α_1 to a conjugate having maximal modulus, we can assume, after relabelling the conjugates of α_1, that α_1 itself has maximal modulus. Then $a\alpha_1 + b\alpha_2 + c\alpha_3 = 0$ gives

$$a|\alpha_1| = |b\alpha_2 + c\alpha_3| \leq (a + b)|\alpha_1|,$$

so that $a \leq b + c$. Similarly $b \leq c + a$ and $\leq a + b$.

A p-adic argument, replacing $|.|$ by $|.|_p$ in the above, gives $|a|_p \leq \max(|b|_p, |c|_p)$. Hence, assuming wlg that $\gcd(a, b, c) = 1$, b and c cannot both be divisible by p. doing this for all primes p, we obtain $\gcd(b, c) = 1$. Similiarly, $\gcd(c, a) = \gcd(a, b) = 1$. Hence a, b and c must satisfy all the conditions of the conjecture.

Conversely, assume that a, b and c satisfy all the conditions of the conjecture, and that the conjecture holds. Take integer solutions (x_i, y_i, z_i) of $ax + by + cz = 0$, as in the conjecture. Then for any numbers β_i, we have $a(\sum_i x_i\beta_i) + b(\sum_i y_i\beta_i) + c(\sum_i z_i\beta_i) = 0$. Now take the β_i to be the roots of $z^n - z - 1 = 0$. The splitting field of this equation has Galois group the full symmetric group S_n. Then condition (*) implies that $\sum_i x_i\beta_i$, $\sum_i y_i\beta_i$ and $\sum_i z_i\beta_i$ are conjugate algebraic integers.

A similar (multiplicative) result concerns solving the equation $x^a y^b z^c = 1$ in conjugate algebraic integers, not roots of unity. (The equation always has a solution in conjugate roots of unity.)

Theorem′. Suppose the conjecture holds. Then the equation $x^a y^b z^c = 1$ has a solution in conjugate algebraic integers that are not roots of unity iff a, b and c satisfy the conditions in the conjecture.

The proof is very similar to the additive case. In the converse part of the proof, we have $(\prod_i \beta_i^{x_i})^a \cdot (\prod_i \beta_i^{y_i})^b \cdot (\prod_i \beta_i^{z_i})^c = 1$, where $\prod_i \beta_i^{x_i}$, $\prod_i \beta_i^{y_i}$ and $\prod_i \beta_i^{z_i}$ are conjugate.

Generalisation to k variables.

General Conjecture. We are given positive integers $a_1, \ldots, a_k$, such that the gcd of any $k-1$ of them is 1 and ans such that the sum of any $k-1$ of them is at least as large as the remaining one. Then there exists a finite number, n say, of integer solutions $(x_{i1}, x_{i2}, \ldots, x_{ik}) \neq (0, 0, \ldots, 0)$ $(i = 1, \ldots, n)$ of $a_1x_1 + \cdots + a_kx_k = 0$ such that

$$\{x_{1j}, \ldots, x_{nj}\}$$

is the same multiset for all $j = 1, 2, \ldots, k$.

Reference.

Smyth, C. J. Additive and multiplicative relations connecting conjugate algebraic numbers. J. Number Theory **23** (1986), 243–254.