Unit equations on quaternions

Yifeng Huang

University of British Columbia

1910.13250, Quaterly Journal of Math. (advised by Michael Zieve)

Let R be a ring. A unit equation is an equation of the form

$$x + y = 1,$$

where x, y ranges over some subsets of R "arising from multiplication" (subject to further specification). Thus, a unit equation is an interplay between the addition structure and the multiplication structure of R.

Example

What are the solutions of

$$\pm 2^m \pm 3^n = 1, m, n \in \mathbb{Z}?$$

$2 - 1 = 1, -2 + 3 = 1, 4 - 3 = 1, -8 + 9 = 1.$
Nontrivial fact: they are all.

An unit equation theorem is a theorem stating that

$$x + y = 1$$

has at most finitely many solutions, assuming some conditions on the sets that x, y range over. There is an ocean of such theorems.

Theorem (Siegel, Mahler '20s–'30s, Parry '50s)

...when x, y are S-units in a number field, where S is a finite set of primes.

For this historical reason, a common name of unit equation theorems found in literature is S-unit theorems.

Theorem (Lang '60)

...when x, y are in a finitely generated subgroup of $\mathbb{C}^\times$.

Theorem (Győry '72+, Evertse '84+, ...)

Effect results: Bound on the height of solutions and the number of solutions.

Every known S-unit theorem so far takes place in a (commutative) field of characteristic zero.
One philosophy to view S-unit theorems is that the multiplicatively defined subsets of allowed x, y have a flavor of geometric progressions. Having lots of solutions $x + y = 1$ is a feature of arithmetic progressions.
Multiplication and addition “should” be incompatible, so one shouldn't expect to find arithmetic progression features in geometric progressions.

Slogan

Coincidences may happen, but not infinitely often.

Thus, one can expect that the S-unit theorem still holds even in noncommutative settings.

Question

Can we find S-unit theorems in noncommutative associative rings?

Example

Let $R = \mathrm{Mat}_2(\mathbb{Q})$ be the matrix algebra over $\mathbb{Q}$. Note that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

So a geometric progression happens to be an arithmetic progression. From here, it is easy to construct counterexamples to any reasonable S-unit theorem one can state. For example, $2f - g = 1$ for any

$$f = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, g = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}$$

Takeaway

We should rule out the matrix algebra, namely, we should consider division algebras.

The quaternion algebra $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is a division algebra with $i^2 = j^2 = k^2 = -1, ij = k$. The quaternion algebra is equipped with a multiplicative (archimedean) norm $|a + bi + cj + dk| = \sqrt{a^2 + b^2 + c^2 + d^2}$. Let $\mathbb{H}_a$ be the set of quaternions whose all four coordinates are real algebraic numbers.

Theorem (H., '20)

Let Γ_1, Γ_2 be finitely generated semigroups of $\mathbb{H}_a^\times$ generated by elements of norms > 1. Fix $a, b, a', b' \in \mathbb{H}_a^\times$, and consider the unit equation

$$axa' + byb' = 1, x \in \Gamma_1, y \in \Gamma_2.$$

Then it has only finitely many solutions if Γ_1 is commutative (i.e. contained in a copy of $\mathbb{C} \subseteq \mathbb{H}$).

Typical case: $f_1, f_2, g_1, g_2 \in \mathbb{H}_a$ with norms > 1, $f_1 f_2 = f_2 f_1$. Then a general form for x, y is

$$x = f_1^{n_1} f_2^{n_2}, n_1, n_2 \geq 0$$

$$y = \text{word in } g_1, g_2 \text{ but not involving } g_1^{-1}, g_2^{-1}$$

Comments

- First noncommtative result.
- Is effective (there are effectively computable bounds on the exponents).
- Uses the Baker's method involving linear forms in logarithms.
- Only requires the archimedean norm. (A main difficulty in the noncommutative setting is that p-adic norms are no longer available, possibly except finitely many.)

An S-unit theorem on a suitable ring has natural consequences in arithmetic dynamics.

- A: an abelian variety.
- $\mathrm{End}(A)$: the endomorphism ring.
- Exponentiation in $\mathrm{End}(A)$ is iteration of a self-map.
- Addition in $\mathrm{End}(A)$ corresponds to translation using the group structure.

So it makes sense that an S-unit theorem on $\mathrm{End}(A)$ says something about iteration of self-maps on A.

Theorem (H., '20, corollary of main theorem)

Let X *be an abelian variety with origin* O *defined over* $k = \overline{k}$*. Assume* $\mathrm{End}(X)$ *lies in a quaternion algebra (for example, when* X *is a supersingular elliptic curve over a finite field). Let* f, g *be self-maps on* X *of degree at least* 2*. (They may not fix* O*.) Let* $O_f(A) := \{A, f(A), f^2(A), \ldots\}$ *denote the forward orbit. Then if there are* $A, B \in X(\overline{k})$ *such that*

$$\#O_f(A) \cap O_g(B) = \infty,$$

then there are $m, n > 0$ *such that* $f^m = g^n$*.*

Slogan

Coincidences may happen, but not infinitely often.

If $\mathrm{End}(X) \subseteq \mathbb{C}$, then the classical S-unit theorem suffices; this case is proven by O'desky–Zieve '19. The case where $\mathrm{End}(X) \subseteq \mathbb{H}_a$ motivates the S-unit theorem on quaternions.

Main theorem recap

Theorem (H., '20)

Let Γ_1, Γ_2 *be finitely generated semigroups of* $\mathbb{H}_a^\times$ *generated by elements of norms* > 1. *Fix* $a, b, a', b' \in \mathbb{H}_a^\times$, *and consider the unit equation*

$$axa' + byb' = 1, x \in \Gamma_1, y \in \Gamma_2.$$

Then it has only finitely many solutions if Γ_1 *is commutative (i.e. contained in a copy of* $\mathbb{C} \subseteq \mathbb{H}$*).*

Intermediate step

Theorem (H., '20)

To prove the main theorem, it suffices to prove

$$|axa'| = |1 - axa'|, x \in \Gamma_1$$

has only finitely many solutions.

I have only proved this for commutative Γ_1. Any other semigroups that satisfy the above statement would generalize the main theorem.

Even the following statement is open. Any progress would be very interesting.

Problem

Let f_1, f_2 be noncommutative elements of $\mathbb{H}_a^\times$ of norms > 1. Fix $a, a' \in \mathbb{H}_a^\times$. Can you find cases of such f_1, f_2, a, a' so that

$$|axa'| = |1 - axa'|, x \in \{f_1^{n_1} f_2^{n_2} : n_1, n_2 \geq 0\}$$

provably has only finitely many solutions?

Thank you!