NORM POLYNOMIAL EQUATIONS WITH MANY SOLUTIONS

P. Moree
C. L. Stewart
R. Tijdeman
J.-H. Evertse

Debrecen, October 26, 2001.

GENERALISED RAMANUJAN-NAGELL EQUATIONS

Consider

(1) $|f(x)| = p_1^{z_1} \cdots p_s^{z_s}$
in $x, z_1, \ldots, z_s \in \mathbb{Z}$

with $f \in \mathbb{Z}[X]$ and with $p_1, p_2, \ldots, p_s$ distinct primes

(E., 1996). If f is irreducible and $\deg f =: r \geq 2$, then the number of solutions of (1) is at most

$$(10^5 r)^{s+1}.$$

LOWER BOUNDS:

(Erdős, Stewart, Tijdeman, 1988)
Let $r \geq 2$, $\varepsilon > 0$. Then for all $S \geq S_0^{\text{ineff}}(r, \varepsilon)$ there are primes $p_1, \ldots, p_S$ and a polynomial $f \in \mathbb{Z}[X]$ of degree r with r distinct zeros in $\mathbb{Q}$, such that

(1) $|f(x)| = p_1^{z_1} \cdots p_S^{z_S}$

has at least

$$\exp\{(1-\varepsilon) r^2 S^{\frac{1}{r}} (\log S)^{\frac{1}{r}-1}\}$$

solutions in $x, z_1, \ldots, z_S \in \mathbb{Z}$.

(Moree, Stewart, 1990)

Let K be a number field of degree $r \geq 2$ and let $\varepsilon > 0$. Then for all $S \geq S_1^{\text{ineff}}(K, \varepsilon)$ there are primes $p_1, \ldots, p_S$ and a polynomial $f \in \mathbb{Z}[X]$ of degree r which is irreducible and has a zero in K, such that

(1) $|f(x)| = p_1^{z_1} \cdots p_S^{z_S}$

has at least

$$\exp\{(1-\varepsilon) r \cdot S^{\frac{1}{r}} (\log S)^{\frac{1}{r}-1}\}$$

solutions in $x, z_1, \ldots, z_S \in \mathbb{Z}$

NORM FORM EQUATIONS

Let K be a number field
$\mathcal{O}_K$ ring of integers

$\alpha_0, \alpha_1, \dots, \alpha_m \in \mathcal{O}_K$
$p_1, \dots, p_s$ distinct prime numbers

Consider

$$(2) \quad |N_{K/\mathbb{Q}}(\alpha_0 x_0 + \alpha_1 x_1 + \dots + \alpha_m x_m)| = p_1^{z_1} \cdots p_s^{z_s}$$

in $x_0, x_1, \dots, x_m, z_1, \dots, z_s \in \mathbb{Z}$.

(Schmidt, Schlickewei, 1970's.)
If $\{\alpha_0, \alpha_1, \dots, \alpha_m\}$ is non-degenerate then (2) has only finitely many solutions with $\gcd(x_0, x_1, \dots, x_m) = 1$

NORM POLYNOMIAL EQUATIONS

K number field, $[K:\mathbb{Q}] = r$
$\alpha_0, \alpha_1, \dots, \alpha_m \in \mathcal{O}_K$, $m < r$
$p_1, \dots, p_s$ distinct primes.

Consider

$$(3) \quad |N_{K/\mathbb{Q}}(\alpha_0 + \alpha_1 X_1 + \dots + \alpha_m X_m)| = p_1^{z_1} p_2^{z_2} \cdots p_s^{z_s}$$

in $X_1, X_2, \dots, X_m, z_1, \dots, z_s \in \mathbb{Z}$

(Bérczes, Győry, to appear)

Suppose $\{\alpha_0, \alpha_1, \dots, \alpha_m\}$ is $\mathbb{Q}$-linearly independent. Then (3) has at most

$$(2^{17} \cdot r)^{\frac{4}{3}(m+2)^3(s+1)}$$

solutions

LOWER BOUNDS

Theorem 1 (MSTE, to appear)

- K number field of degree $r \geq 2$
- $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathcal{O}_K$ $\mathbb{Q}$-linearly independent, $m < r$
- $\varepsilon > 0$.

Then for every $S \geq S_0^{\text{eff}}(K, \varepsilon, \alpha_1, \dots, \alpha_m)$ there are primes $p_1, \dots, p_S \in \mathbb{Z}$ and $\alpha_0 \in \mathcal{O}_K$ such that

- α_0 is $\mathbb{Q}$-linearly independent of $\alpha_1, \dots, \alpha_m$
- $|N_{K/\mathbb{Q}}(\alpha_0 + \alpha_1 x_1 + \dots + \alpha_m x_m)| = p_1^{z_1} \cdots p_S^{z_S}$

has at least

$$\exp\{(1-\varepsilon)\tfrac{r}{m} S^{\frac{m}{r}} (\log S)^{\frac{m}{r}-1}\}$$

solutions in $x_1, \dots, x_m, z_1, \dots, z_S \in \mathbb{Z}$.

For $\alpha_0, \alpha_1, \dots, \alpha_m \in \mathcal{O}_K$ and primes $p_1, \dots, p_S \in \mathbb{Z}$, let $g(\alpha_0, \dots, \alpha_m, p_1, \dots, p_S)$ be the smallest integer g with the following property:

There exists a polynomial $F \in \bar{\mathbb{Q}}[X_1, \dots, X_m]$ of total degree g such that every solution $(x_1, \dots, x_m, z_1, \dots, z_S) \in \mathbb{Z}^{m+S}$ of

$$|N_{K/\mathbb{Q}}(\alpha_0 + \alpha_1 x_1 + \dots + \alpha_m x_m)| = p_1^{z_1} \cdots p_S^{z_S} \tag{3}$$

satisfies $F(x_1, \dots, x_m) = 0$.

(i.e. the points $(x_1, \dots, x_m) \in \mathbb{Z}^m$ satisfying (3) for some $z_1, \dots, z_S \in \mathbb{Z}$ do not lie in a hypersurface of degree $< g$).

Theorem 2 (MSTE, to appear)

Let $K, r, m, \varepsilon, \alpha_1, \dots, \alpha_m$ as in Theorem 1.

Then for every $S \geq S_1^{\text{eff}}(K, \varepsilon, \alpha_1, \dots, \alpha_m)$ there are primes $p_1, \dots, p_S \in \mathbb{Z}$ and $\alpha_0 \in \mathcal{O}_K$ such that

- α_0 is $\mathbb{Q}$-linearly independent of $\alpha_1, \dots, \alpha_m$
- $g(\alpha_0, \alpha_1, \dots, \alpha_m, p_1, \dots, p_S)$

$$\geq \exp\{(1-\varepsilon) r \cdot S^{\frac{1}{r}} (\log S)^{\frac{1}{r}-1}\}.$$

MAIN TOOL

K number field
T finite set of prime ideals of $\mathcal{O}_K$

$\Psi_{K,T}(X,Y)$ = number of ideals of $\mathcal{O}_K$ of norm $\leq X$ which are composed of prime ideals that have norm $\leq Y$ and lie outside T.

Theorem 3 (MSTE, to appear)

Let $Y \geq 3$, $u := \frac{\log X}{\log Y} \geq 3$. Then

$$\Psi_{K,T}(X,Y) \geq$$
$$X \cdot \exp\left\{-u\left(\log u + \log\log u - 1 + \frac{\log\log u - 1}{\log u} + C \cdot \left(\frac{\log\log u}{\log u}\right)^2\right)\right\}$$

with $C = C^{\text{eff}}(K,T)$

EXTENSION OF EARLIER RESULTS:

- Canfield, Erdős, Pomerance (1983)
  Similar lower bound for
  $\psi(X,Y) = \Psi_{\mathbb{Q},\emptyset}(X,Y)$ with
  C ineffective (?)

- Krause, Moree (independant, 1989)
  Similar lower bound for
  $\Psi_K(X,Y) = \Psi_{K,\emptyset}(X,Y)$ with
  C ineffective (?)

IDEA OF PROOF OF THEOREM 1

- Let $\alpha_1, \dots, \alpha_m \in \mathcal{O}_K$ be the numbers from Theorem 1.
- Choose $\alpha_{m+1}, \dots, \alpha_{50_K}$ such that $\{\alpha_1, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_r\}$ is a $\mathbb{Q}$-basis of K
- Choose parameters X, Y.
  Let $p_1, \dots, p_s$ be the prime numbers $\le Y$
- Let $\Psi_0(X,Y)$ be the number of tuples $(x_1, x_2, \dots, x_r) \in \mathbb{Z}^r$ such that

- $|x_1|, |x_2|, \dots, |x_r| \le X$
- $\alpha_{m+1} x_{m+1} + \dots + \alpha_r x_r \neq 0$
- $|N_{K/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_r x_r)|$ composed of primes $\le Y$.

Apply box principle:

There is $\alpha_0 := \sum_{i=m+1}^{r} \alpha_i x_i^{(0)}$

with $x_i^{(0)} \in \mathbb{Z}$, $|x_i^{(0)}| \leq X$, $\alpha_0 \neq 0$

such that

$|N_{K/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_m x_m + \alpha_0)|$ is composed of primes $\leq Y$ for at least $\Psi_0(X,Y)/X^{r-m}$ tuples $(x_1, \dots, x_m) \in \mathbb{Z}^m$

$\Longrightarrow$

- α_0 is $\mathbb{Q}$-linearly independent of $\alpha_1, \dots, \alpha_m$
- $|N_{K/\mathbb{Q}}(\alpha_0 + \alpha_1 x_1 + \dots + \alpha_m x_m)| = p_1^{a_1} \cdots p_s^{a_s}$ has at least $\Psi_0(X,Y)/X^{r-m}$ solutions

Lemma

There are a constant c and a finite set of prime ideals T, both effectively depending on $K, \alpha_1, \dots, \alpha_m$, such that

$$\Psi_0(X,Y) \geq c \cdot \Psi_{K,T}(X^r, Y).$$

Now let $Y \to \infty$ and choose X optimally.