Effective Methods for Diophantine Equations

Szabolcs Tengely

tengely@math.leidenuniv.nl

Leiden University

Runge-type Diophantine Equations

Runge's Condition

$$P(X,Y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} X^i Y^j$$

Let $\lambda > 0$.

- $\lambda-$leading part of P, $P_\lambda(X,Y)$, is the sum of all terms $a_{i,j}X^iY^j$ of P for which $i + \lambda j$ is maximal
- the leading part of P, denoted by $\tilde{P}(X,Y)$, is the sum of all monomials of P which appear in any P_λ as λ varies

P satisfies Runge's condition unless there exists a λ so that $\tilde{P} = P_\lambda$ is a constant multiple of a power of an irreducible polynomial in $\mathbb{Q}[X,Y]$

Example

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

Example

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X,Y) = X^2, \quad \lambda < \frac{1}{4}$

Example

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X,Y) = X^2, \quad \lambda < \frac{1}{4}$
- $P_\lambda(X,Y) = X^2 - Y^8, \quad \lambda = \frac{1}{4}$

Example

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X,Y) = X^2, \quad \lambda < \frac{1}{4}$
- $P_\lambda(X,Y) = X^2 - Y^8, \quad \lambda = \frac{1}{4}$
- $P_\lambda(X,Y) = Y^8, \quad \lambda > \frac{1}{4}$

Example

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X,Y) = X^2, \quad \lambda < \frac{1}{4}$
- $P_\lambda(X,Y) = X^2 - Y^8, \quad \lambda = \frac{1}{4}$
- $P_\lambda(X,Y) = Y^8, \quad \lambda > \frac{1}{4}$
- thus $\tilde{P}(X,Y) = X^2 - Y^8 = (X - Y^4)(X + Y^4)$

Runge's theorem

Theorem (Runge,1887). *If* P *satisfies Runge's condition, then the Diophantine equation* $P(x, y) = 0$ *has only a finite number of integer solutions.*

The case $F(x) = G(y)$

$F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n, \deg G = m,$ such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$. Let $d > 1$ be a divisor of $\gcd(n, m)$.

The case $F(x) = G(y)$

$F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n, \deg G = m,$ such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$. Let $d > 1$ be a divisor of $\gcd(n, m)$. Runge's condition is satisfied.

The case $F(x) = G(y)$

$F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n, \deg G = m,$ such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1.$ Let $d > 1$ be a divisor of $\gcd(n, m).$ Runge's condition is satisfied.

Theorem (Sz.T.). *If $(x, y) \in \mathbb{Z}^2$ is a solution of $F(x) = G(y)$ where F and G satisfy the above mentioned conditions then*

$$\max\{|x|, |y|\} \leq d^{\frac{2m^2}{d} - m}(m+1)^{\frac{3m}{2d}}\left(\frac{m}{d}+1\right)^{\frac{3m}{2}}(h+1)^{\frac{m^2+mn+m}{d}+2m},$$

where $h = \max\{H(F), H(G)\}$ and $H(\cdot)$ denotes the classical height, that is the maximal absolute value of the coefficients.

About the proof

Lemma (Walsh,1992). *There exist Puiseux expansions (in this case even Laurent expansions)*

$$u(X) = \sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \text{ and } \quad v(X) = \sum_{i=-\frac{m}{d}}^{\infty} g_i X^{-i}$$

of the algebraic functions U, V *defined by* $U^d = F(X), V^d = G(X)$, *such that* $d^{2(n/d+i)-1} f_i \in \mathbb{Z}$ *for all* $i > -\frac{n}{d}$, *similarly* $d^{2(m/d+i)-1} g_i \in \mathbb{Z}$ *for all* $i > -\frac{m}{d}$, *and* $f_{-\frac{n}{d}} = g_{-\frac{m}{d}} = 1$. *Furthermore* $|f_i| \leq (H(F)+1)^{\frac{n}{d}+i+1}$ *for* $i \geq -\frac{n}{d}$ *and* $|g_i| \leq (H(G)+1)^{\frac{m}{d}+i+1}$ *for* $i \geq -\frac{m}{d}$.

$$F(X) = \left(\sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \right)^d , \quad G(Y) = \left(\sum_{i=-\frac{m}{d}}^{\infty} g_i Y^{-i} \right)^d ,$$

if $|t|$ is large enough then

$$|\sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} f_i t^{-i}| < \frac{1}{2}$$

and

$$|\sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} g_i t^{-i}| < \frac{1}{2}$$

$F(x) = G(y)$ therefore $u(x)^d - v(y)^d = 0$

$$(u(x) - v(y)) \left(u(x)^{d-1} + u(x)^{d-2} v(y) + \ldots + v(y)^{d-1} \right) = 0,$$

if d is odd,

$$\left(u(x)^2 - v(y)^2\right) \left(u(x)^{d-2} + u(x)^{d-4} v(y)^2 + \ldots + v(y)^{d-2} \right) = 0,$$

if d is even.

$u(x) = v(y)$ if d is odd, and
$u(x) = \pm v(y)$ if d is even.

We conclude that

$$0 = |u(x) \pm v(y)| = \left| \sum_{i=-\frac{n}{d}}^{\infty} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^{\infty} g_i y^{-i} \right|.$$

If $|x|$ and $|y|$ are large enough, then

$$\left| \sum_{i=-\frac{n}{d}}^{0} d^{\frac{2m}{d}-1} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^{0} d^{\frac{2m}{d}-1} g_i y^{-i} \right| < 1.$$

Hence x satisfies

$$\text{Res}_Y(F(X) - G(Y), Q(X,Y)) = 0$$

and y satisfies

$$\text{Res}_X(F(X) - G(Y), Q(X,Y)) = 0,$$

where

$$Q(x,y) := \sum_{i=0}^{\frac{n}{d}} d^{\frac{2m}{d}-1} f_{-i} x^i \pm \sum_{i=0}^{\frac{m}{d}} d^{\frac{2m}{d}-1} g_{-i} y^i = 0.$$

Algorithm

Let $u(X) = \sum_{i=-\frac{n}{p}}^{0} f_i X^{-i}$ and $v(X) = \sum_{i=-\frac{m}{p}}^{0} g_i X^{-i}$. Let t be a positive real number. Suppose that p is odd. Then we have

$$(u(x) - t)^p < F(x) < (u(x) + t)^p \text{ for } x \notin [x_t^-, x_t^+],$$
$$(v(y) - t)^p < G(y) < (v(y) + t)^p \text{ for } y \notin [y_t^-, y_t^+],$$

where

$$x_t^- = \min\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0 \text{ or } F(x) - (u(x) + t)^p = 0\}\},$$
$$x_t^+ = \max\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0 \text{ or } F(x) - (u(x) + t)^p = 0\}\}.$$

We have

$$u(x) - t < F(x)^{1/p} < u(x) + t \text{ for } x \notin [x_t^-, x_t^+],$$
$$v(y) - t < G(y)^{1/p} < v(y) + t \text{ for } y \notin [y_t^-, y_t^+],$$

hence

$$|u(x) - v(y)| < 2t.$$

Hence x is a solution of $\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T)$ for some rational number $-2t < T < 2t$ with denominator dividing $p^{\frac{2m}{p}-1}$.

$F(x) = G(k)$ for some $k \in [y_t^-, y_t^+]$,

$G(y) = F(k)$ for some $k \in [x_t^-, x_t^+]$,

$\text{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T) = 0$ for some

$T \in \mathbb{Q}, |T| < 2t$ with denominator dividing D.

The number of equations to be solved depends on t, a good choice can reduce the time of the computation. We let $t = \frac{1}{2D}$. In this way if $x \notin [x_t^-, x_t^+], y \notin [y_t^-, y_t^+]$, we have that

$$-1 < D(u(x) \pm v(y)) < 1.$$

Since $D(u(x) \pm v(y))$ is an integer the only possibility is $u(x) \pm v(y) = 0$. In this case there is only one resultant equation to be solved if p is odd and two if $p = 2$.

Example

We apply the method to the Diophantine equation $F(x) = G(y)$, where

$$F(x) = x^3 - 5x^2 + 45x - 713,$$

$$G(y) = y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y.$$

We obtain that

$$u(X) = X - \frac{5}{3},$$

$$v(Y) = Y^3 - Y^2 + 2Y - \frac{4}{3}.$$

t	#equations	$[x_t^-, x_t^+, y_t^-, y_t^+]$
1/6	177	[-86, 45, -32, 11]
1/3	95	[-48, 15, -18, 9]
2/3	67	[-27, 13, -10, 8]
4/3	52	[-16, 11, -2, 6]

$\text{Res}_Y(F(X) - G(Y), u(X) - v(Y) - k) = 0,$

for $k \in \{-7, \ldots, 7\}$,

$G(y) = F(x),$ for $x \in \{-16, \ldots, 11\}$,

$F(x) = G(y),$ for $y \in \{-2, \ldots, 6\}$,

The Diophantine equation $x^2 + q^{2m} = 2y^p$

Consider the Diophantine equation

$$x^2 + q^{2m} = 2y^p,$$

where $x, y \in \mathbb{N}$ with $\gcd(x, y) = 1, m \in \mathbb{N}$ and p, q are odd primes and $\mathbb{N}$ denotes the set of positive integers. The case $m = 0$ was solved by Cohn in 1996.

Theorem (Sz.T.). *There are only finitely many solutions* (x, y, m, q, p) *of* $x^2 + q^{2m} = 2y^p$ *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not of the form* $2v^2 \pm 2v + 1, m \in \mathbb{N}$ *and* $p > 3, q$ *odd primes.*

Be careful examples

y	p	q
5	13	42641
5	29	1811852719
5	97	2299357537036323025594528471766399
13	7	11003
13	13	13394159
25	11	69049993
25	47	378293055860522027254001604922967
41	31	4010333845016060415260441

Solutions with small q^m

Lemma (Sz.T.). *Let* q *be an odd prime and* $m \in \mathbb{N}$ *such that* $3 \leq q^m \leq 501$. *If there exist* $(x, y) \in \mathbb{N}^2$ *with* $\gcd(x, y) = 1$ *and an odd prime* p *such that* $x^2 + q^{2m} = 2y^p$ *holds, then*

$$(x, y, q, m, p) \in \Big\{(3, 5, 79, 1, 5), (9, 5, 13, 1, 3), (55, 13, 37, 1, 3), (79, 5, 3, 1, 5), (99, 17, 5, 1, 3), (161, 25, 73, 1, 3), (249, 5, 307, 1, 7), (351, 41, 11, 2, 3), (545, 53, 3, 3, 3), (649, 61, 181, 1, 3), (1665, 113, 337, 1, 3), (2431, 145, 433, 1, 3), (5291, 241, 19, 1, 3), (275561, 3361, 71, 1, 3)\Big\}.$$

$\mathbb{Z}[i]$ is a unique factorization domain.

$$x = \Re((1+i)(u+iv)^p) =: F_p(u,v),$$
$$q^m = \Im((1+i)(u+iv)^p) =: G_p(u,v).$$

Lemma (Sz.T.). *We have*

$$(u - \delta_4 v) \quad | \quad F_p(u,v),$$
$$(u + \delta_4 v) \quad | \quad G_p(u,v),$$

where

$$\delta_4 = \begin{cases} 1 \textit{ if } p \equiv 1 \pmod 4, \\ -1 \textit{ if } p \equiv 3 \pmod 4. \end{cases}$$

Either

$$u + \delta_4 v = q^k,$$
$$H_p(u, v) = q^{m-k},$$

or

$$u + \delta_4 v = -q^k,$$
$$H_p(u, v) = -q^{m-k},$$

where $H_p(u, v) = \frac{G_p(u,v)}{u+\delta_4 v}$ and $0 \leq k \leq m$.

Lemma (Mignotte,2001). *Let* α *be a complex algebraic number with* $|\alpha| = 1$, *but not a root of unity, and* $\log \alpha$ *the principal value of the logarithm. Put* $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]/2$. *Consider the linear form*

$$\Lambda = b_1 i\pi - b_2 \log \alpha,$$

where b_1, b_2 *are positive integers. Let* λ *be a real number satisfying* $1.8 \leq \lambda < 4$, *and put*

$$\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2),$$

$$t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1 + 2\pi\rho/3\lambda)}, \quad T = \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda}\right)^2,$$

$$H = \max\left\{3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho} + \frac{1}{2K}\right) - \log\sqrt{T} + 0.886\right) + \right.$$

$$\left. + \frac{3\lambda}{2} + \frac{1}{T}\left(\frac{1}{6\rho\pi} + \frac{1}{3K}\right) + 0.023\right\}.$$

Then

$$\log|\Lambda| > -(8\pi T\rho\lambda^{-1}H^2 + 0.23)K - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

Bound for p

Theorem (Sz.T.). *If the equation $x^2 + q^{2m} = 2y^p$ admits a relatively prime solution $(x, y) \in \mathbb{N}^2$ then we have*

$$p \leq 3803 \text{ if } u + \delta_4 v = \pm q^m, q^m \geq 503,$$
$$p \leq 3089 \text{ if } p = q,$$
$$p \leq 1309 \text{ if } u + \delta_4 v = \pm q^m, m \geq 40,$$
$$p \leq 1093 \text{ if } u + \delta_4 v = \pm q^m, m \geq 100,$$
$$p \leq 1009 \text{ if } u + \delta_4 v = \pm q^m, m \geq 250.$$

Without loss of generality we assume that $p > 1000$ and $q^m \geq 503$. Proof in the case $u + \delta_4 v = \pm q^m, q^m \geq 503$. From $u + \delta_4 v = \pm q^m$ we get

$$\frac{503}{2} \leq \frac{q^m}{2} \leq \frac{|u| + |v|}{2} \leq \sqrt{\frac{u^2 + v^2}{2}} = \sqrt{\frac{y}{2}},$$

which yields that $y \geq \frac{q^{2m}}{2} > 126504.$

W

e have

$$\left|\frac{x+q^m i}{x-q^m i}-1\right| = \frac{2\cdot q^m}{\sqrt{x^2+q^{2m}}} \le \frac{2\sqrt{y}}{y^{p/2}} = \frac{2}{y^{\frac{p-1}{2}}}.$$

and

$$\frac{x+q^m i}{x-q^m i} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\left(\frac{u+iv}{u-iv}\right)^p.$$

Lemma (Sz.T.). *The polynomial* $H_p(\pm q^k - \delta_4 v, v)$ *has degree* $p-1$ *and*

$$H_p(\pm q^k - \delta_4 v, v) = \pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^k p \widehat{H}_p(v) + q^{k(p-1)},$$

where $\widehat{H}_p \in \mathbb{Z}[X]$ *has degree* $< p-1$. *The polynomial* $H_p(X,1) \in \mathbb{Z}[X]$ *is irreducible and*

$$H_p(X,1) = \prod_{\substack{k=0\\k\neq k_0}}^{p-1} \left(X - \tan\frac{(4k+3)\pi}{4p} \right),$$

where $k_0 = \left[\frac{p}{4}\right] \ (p \mod 4)$.

Lemma (Sz.T.). *If there exists a* $k \in \{0, 1, \ldots, m\}$ *such that*

$$u + \delta_4 v = q^k,$$
$$H_p(u, v) = q^{m-k},$$

or

$$u + \delta_4 v = -q^k,$$
$$H_p(u, v) = -q^{m-k},$$

has a solution $(u, v) \in \mathbb{Z}^2$ *with* $\gcd(u, v) = 1$*, then either* $k = 0$ *or* $k = m, p \neq q$ *or* $(k = m - 1, p = q)$.

Proof of the finiteness result

We have that $k = 0, m - 1$ or $k = m$.

Proof of the finiteness result

We have that $k = 0, m - 1$ or $k = m$.

- If $k = 0$, then $u + \delta_4 v = \pm 1$ and $y = 2v^2 \pm 2v + 1$.

Proof of the finiteness result

We have that $k = 0, m-1$ or $k = m$.

- If $k = 0$, then $u + \delta_4 v = \pm 1$ and $y = 2v^2 \pm 2v + 1$.
- If $k = m-1$, then $p = q$ and we have $p < 3089$. We recall that $H_p(u,v)$ is an irreducible polynomial of degree $p-1$. Thus we have only finitely many Thue equations

$$H_p(u,v) = \pm p.$$

Proof of the finiteness result

We have that $k = 0, m-1$ or $k = m$.

- If $k = 0$, then $u + \delta_4 v = \pm 1$ and $y = 2v^2 \pm 2v + 1$.
- If $k = m - 1$, then $p = q$ and we have $p < 3089$. We recall that $H_p(u, v)$ is an irreducible polynomial of degree $p - 1$. Thus we have only finitely many Thue equations

$$H_p(u, v) = \pm p.$$

- Let $k = m$. Here we have $u + \delta_4 v = \pm q^m$ and $H_p(\pm q^m - \delta_4 v, v) = \pm 1$. If $q^m \leq 501$ then there are only finitely many solutions. We have computed an upper bound for p when $q^m \geq 503$. This leads to finitely many Thue equations

$$H_p(u, v) = \pm 1.$$

Fixed y

Theorem (Sz.T.). *The only solution* (m, p, q, x) *in positive integers* m, p, q, x *with* p *and* q *odd primes of the equation* $x^2 + q^{2m} = 2 \cdot 17^p$ *is* $(1, 3, 5, 99)$.

Proof. Note that 17 is not of the form $2v^2 \pm 2v + 1$. From $y = u^2 + v^2$ we obtain that q is 3 or 5 and $m = 1$. This implies that 17 does not divide x. We are left with the equations

$$x^2 + 3^2 = 2 \cdot 17^p,$$
$$x^2 + 5^2 = 2 \cdot 17^p.$$

We saw that there is no solution with $q = 3, m = 1, y = 17$ and the only solution in case of the second equation is $(x, y, q, m, p) = (99, 17, 5, 1, 3)$. $\square$

Fixed q

Theorem (Sz.T.). *If the Diophantine equation* $x^2 + 3^m = 2y^p$ *with* $m > 0$ *and* p *prime admits a coprime integer solution* (x, y), *then either*

$$p \in \{3, 59, 83, 107, 179, 227, 347, 419, \\ 443, 467, 563, 587, 659, 683, 827, 947\}$$

or $(x, y, m, p) = (79, 5, 2, 5)$.

Mixed powers in arithmetic progressions

Let $x_0^3, x_1^2, x_2^3, x_3^2$ be consecutive terms of an arithmetic progression. We have

$$x_1^2 = \frac{x_0^3 + x_2^3}{2},$$
$$x_3^2 = \frac{-x_0^3 + 3x_2^3}{2}.$$

We note that $x_2 = 0$ implies $x_0 = x_1 = x_2 = x_3 = 0$. Assume $x_2 \neq 0$. Then we obtain that

$$\left(\frac{2x_1x_3}{x_2^3}\right)^2 = -\left(\frac{x_0}{x_2}\right)^6 + 2\left(\frac{x_0}{x_2}\right)^3 + 3.$$

Theorem. *Let* $\mathcal{C}$ *be the curve given by*

$$Y^2 = -X^6 + 2X^3 + 3.$$

Then $\mathcal{C}(\mathbb{Q}) = \{(-1,0),(1,\pm 2)\}$.

Corollary. *If* $x_0^3, x_1^2, x_2^3, x_3^2$ *are consecutive terms of an arithmetic progression, then* $(x_0,x_1,x_2,x_3) \in \{(-2t^2, 0, 2t^2, \pm 4t^3), (t^2, \pm t^3, t^2, \pm t^3)\}$ *for some* $t \in \mathbb{Z}$.

Proof. The point $(-1,0)$ is on the curve $Y^2 = -X^6 + 2X^3 + 3$, hence $\frac{x_0}{x_2} = -1$ and $2x_1x_3 = 0$. It easily follows that $x_0 = -2t^2, x_1 = 0, x_2 = 2t^2, x_3 = \pm 4t^3$ is the only possible solution of the problem. In case of the other two points $(1,\pm 2)$ we have $x_0 = x_2$, which implies $x_0^3 = x_1^2 = x_2^3 = x_3^2$. Thus $x_0 = x_2 = t^2$ and $x_1 = x_3 = \pm t^3$ for some $t \in \mathbb{Z}$. □