On approximation of real, complex, and p-adic numbers by algebraic numbers of bounded degree

Today we will discuss the problem of approximation of real, complex, and p-adic numbers by algebraic numbers. The problem of approximation to real numbers is of classical interest in the theory of Diophantine approximation.

In 1842 Dirichlet proved that *for any real irrational number ξ there exist infinitely many rational numbers p/q such that*

$$\left|\xi - \frac{p}{q}\right| < q^{-2}. \tag{1}$$

Multiplying (1) by q, we get

$$|q\xi - p| < q^{-1},$$

and so we obtain the polynomial interpretation of Dirichlet's Theorem: *For any real irrational number ξ there exist infinitely many integer polynomials P of the first degree such that*

$$|P(\xi)| \ll \lceil P \rceil^{-1},$$

where $\lceil P \rceil$ denote the height of the polynomial P, that is the maximum of absolute values of its coefficients, $\ll$ is the Vinogradov symbol. Using Dirichlet's box principle it is easy to prove a more general statement, namely: *For any real number $\xi \notin \mathbb{A}_n$ there exist infinitely many integer polynomials P of degree $\leq n$ such that*

$$|P(\xi)| \ll \lceil P \rceil^{-n},$$

where $\mathbb{A}_n$ is the set of real algebraic numbers of degree $\leq n$. It is very natural to suppose, that (1) can also be generalized to the case of approximation by algebraic numbers of degree $\leq n$. But this problem turns out to be very difficult.

In 1961 E. Wirsing made the following

Conjecture (Wirsing, 1961). *For any real number $\xi \notin \mathbb{A}_n$ there exist infinitely many algebraic numbers $\alpha \in \mathbb{A}_n$ with*

$$|\xi - \alpha| \leq c\, H(\alpha)^{-A}, \tag{2}$$

where

$$A = n + 1 - \epsilon,$$

and $H(\alpha)$ is the height of α, $\epsilon > 0$, and $c = c(\xi, n, \epsilon)$.

In 1965 V. Sprindžuk proved that the Conjecture of Wirsing holds for almost all real numbers. Further W. M. Schmidt conjectured that the exponent $n + 1 - \epsilon$ can be replaced even by $n + 1$. In 1967 H. Davenport and W. Schmidt proved the Conjecture for algebraic numbers of degree ≤ 2, $A = 3$. However, until now we don't know how to solve this problem for $n > 3$.

In his paper E. Wirsing proved that (2) holds for

$$A = \frac{n}{2} + \frac{3}{2}. \tag{3}$$

At the end of the paper he slightly refined this result. Now I want to explain his method. But first I exhibit difficulties which occur when we try to prove the Conjecture, for example, for $n = 2$. Using Dirichlet's Box principle for any $H > 0$ we can construct an integer polynomial

$$P(x) = a_2 x^2 + a_1 x + a_0 = a_2(x - \alpha_1)(x - \alpha_2)$$

such that

$$|P(\xi)| \ll H^{-2}, \quad \overline{|P|} \ll H,$$

We can rewrite this expression as

$$|\xi - \alpha_1||\xi - \alpha_2| \ll H^{-2} a_2^{-1}.$$

And now see: Even if $a_2 = H$, we can only prove that

$$|\xi - \alpha_1||\xi - \alpha_2| \ll H^{-3},$$

or

$$\min(|\xi - \alpha_1|,\ |\xi - \alpha_2|) \ll H^{-\frac{3}{2}}.$$

Therefore, using Dirichlet's method we can only prove that for any real number ξ there exist infinitely many algebraic numbers α of degree ≤ 2 such that

$$|\xi - \alpha| \ll H(\alpha)^{-\frac{3}{2}}.$$

It is easy to verify that if we consider the polynomial P of the n-th degree, we can only obtain an estimation

$$|\xi - \alpha| \ll H(\alpha)^{-1-\frac{1}{n}}, \tag{4}$$

which is very weak. It is also clear, that the worth case for us is when

$$|\xi - \alpha_1| = \ldots = |\xi - \alpha_n| \ll H^{-1-\frac{1}{n}}, \tag{5}$$

that is when all roots of the polynomial P are very closed to ξ. And now the question is: is it possible to move aside some of these roots from ξ? Or: is it possible to prove that situation (5) is impossible? The answer is 'Yes', and the basic idea of Wirsing's proof is as follows:

Using Dirichlet's Box principle for any $H > 0$ one can construct integer polynomials

$$P(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 = a_\ell(\xi - \alpha_1) \cdot \ldots \cdot (\xi - \alpha_\ell), \quad 1 \leq \ell \leq n,$$

$$Q(x) = b_m x^m + \ldots + b_1 x + b_0 = b_m(\xi - \beta_1) \cdot \ldots \cdot (\xi - \beta_m), \quad 1 \leq m \leq n,$$

which have no common root such that

$$\begin{aligned} &|a_\ell| \ll H, \quad \ldots, \quad |a_0| \ll H, \quad |P(\xi)| \ll H^{-n}, \\ &|b_m| \ll H, \quad \ldots, \quad |b_0| \ll H, \quad |Q(\xi)| \ll H^{-n}. \end{aligned} \tag{6}$$

Moreover, the interesting case for us is when $\ell, m > 1$, since in the opposite case we have just the polynomial of the first degree and therefore

$$|\xi - \alpha| \ll H(\alpha)^{-n-1}$$

by (6). We now consider the resultant $R(P, Q)$. On the one hand, since P and Q are integer polynomials and have no common root, we have

$$1 \leq |R(P, Q)|.$$

On the other hand,

$$1 \le R(P,Q) \quad = a_\ell^m b_m^\ell \prod_{i,\ j} (\alpha_i - \beta_j) \ll H^{m+\ell} \prod_{i,\ j} (\alpha_i - \beta_j). \tag{7}$$

Now suppose that (5) is valid. Substituting this into (7), we get:

$$1 \ll H^{m+\ell} \prod_{i,\ j} (\alpha_i - \beta_j) \ll H^{m+\ell} H^{-\left(1+\frac{1}{n}\right)m\ell} \ll H^{m+\ell-\left(1+\frac{1}{n}\right)m\ell} \le H^{-\frac{4}{n}},$$

which is impossible if H is sufficiently large.

More precise consideration of (7) enables us to derive the following formula:

$$|\xi - \alpha| \ll \max \begin{cases} |P(\xi)|^{1/2} |Q(\xi)| H^{n-3/2}, \\ |P(\xi)| |Q(\xi)|^{1/2} H^{n-3/2}, \end{cases} \tag{8}$$

where α is the root of P or Q closest to ξ. If we substitute (6) into (8), we get

$$|\xi - \alpha| \ll H^{-n/2-n+n-3/2} = H^{-n/2-3/2}, \tag{9}$$

which gives (3).

This method is quite understandable. But! After 1961 during a long period there were no ideas or methods, which allow to improve this result with the only exception of H. Davenport and W.M. Schmidt's Theorem.

In 1993 V. Bernik and K. Tishchenko obtained the following result:

$$A = \frac{n}{2} + \gamma_n, \quad \lim_{n\to\infty} \gamma_n = 3.$$

The idea is as follows: Using Dirichlet's Box principle for any $H > 0$ one can construct integer polynomials P and Q such that

$$\begin{aligned} &|a_n| \ll H, \quad \dots, \quad |a_2| \ll H, \quad |a_1| \ll H^{1+\epsilon}, \quad |a_0| \ll H^{1+\epsilon}, \quad |P(\xi)| \ll H^{-n-\epsilon}, \\ &|b_n| \ll H, \quad \dots, \quad |b_2| \ll H, \quad |b_1| \ll H^{1+\epsilon}, \quad |b_0| \ll H^{1+\epsilon}, \quad |Q(\xi)| \ll H^{-n-\epsilon}, \end{aligned} \tag{10}$$

where $\epsilon > 0$. We now consider two cases:

Case A: Let

$$\max(|a_1|,\ |a_0|,\ |b_1|,\ |b_0|) \ll H.$$

Then we can apply (8). Substituting (10) into (8), we get:

$$|\xi - \alpha| \ll H(\alpha)^{-n/2-3/2-3\epsilon/2}, \tag{11}$$

which is better then (9).

Case B: Let

$$\max(|a_1|,\ |a_0|,\ |b_1|,\ |b_0|) \gg H,$$

that is

$$\max(a_1,\ a_0,\ b_1,\ b_0) = H^{1+\delta} = \overline{|P|},$$

where $0 < \delta \leq \epsilon$. It is clear that in this case the derivative of P or Q (or both) is "big", that is

$$|P'(\xi)| \asymp H^{1+\delta}. \tag{12}$$

We have the following well-known inequality

$$|\xi - \alpha| \ll \frac{|P(\xi)|}{|P'(\xi)|}, \tag{13}$$

where α is the root of the polynomial P closest to ξ. Substituting (10) and (12) into (13), we get

$$|\xi - \alpha| \ll \frac{H^{-n-\epsilon}}{H^{1+\delta}} = H^{-n-\epsilon-1-\delta} = H^{-(1+\delta)\frac{n+1+\epsilon+\delta}{1+\delta}} \ll H(\alpha)^{-\frac{n+1+\epsilon+\delta}{1+\delta}} \ll H(\alpha)^{-\frac{n+1+2\epsilon}{1+\epsilon}}. \tag{14}$$

Now see: If we take $\epsilon = 0$, then

$$|\xi - \alpha| \ll H(\alpha)^{-n-1},$$

which is very strong. BUT! In this case, (11) is weak. On the other hand, if we take $\epsilon = 1$, then (11) looks like nice, but (14) is weak. Finally, if we choose an optimal value of ϵ, namely

$$\epsilon = 1 - \frac{6}{n},$$

we obtain

$$|\xi - \alpha| \ll H(\alpha)^{-n/2+\gamma_n}, \quad \lim_{n\to\infty} \gamma_n = 3,$$

in both cases.

One can say: "It's very easy to improve also this result. Let's consider (10), but with three "big" coefficients. In this case $|P(\xi)|,\ |Q(\xi)| \ll H^{-n-2\epsilon}$ and the result will be definitely better. " Unfortunately, this trick does not work. And the reason is: since P has three "big" coefficients, its derivative has two "big" coefficients, therefore it can be small. So, (12) is not true.

In 1996 the following approach was found: Let $P^{(k)}$ be a polynomial of (10)-type with k "big" coefficients. Let's consider n polynomials

$$Q,\ P^{(0)},\ P^{(3)}, \ldots, P^{(n)}. \tag{15}$$

One can prove that they are linearly independent. Using linear combination of these polynomials we construct a polynomial

$$L = d_1 Q + d_2 P^{(0)} + d_3 P^{(3)} + \ldots + d_n P^{(n)}$$

with two "big" coefficients. The cases A and B do work for L. Moreover, it is possible to show that an influence of the numbers $d_1, \ldots, d_2$ is very weak, therefore

$$|L(\xi)| \ll H^{-n-2\epsilon}$$

$$\lceil L \rceil \ll H^{1+\epsilon},$$

which gives

$$A = n/2 + \gamma_n, \quad \lim_{n\to\infty} \gamma_n = 4.$$

A deep modification of the construction of the polynomials (15) enabled to obtain the following result:

$$A = n/2 + \gamma_n, \quad \lim_{n\to\infty} \gamma_n = \infty.$$

At the moment this paper is in preparation. I also want to stress that the idea to consider linearly independent polynomials and to construct a new polynomial of a special type was taken from the paper of H. Davenport and W.M. Schmidt (1967).

It is also very interesting to consider complex and p-adic analogues of these results. The history of these questions is rather pure than the previous one. The most recent result about approximation of complex numbers is:

$$A = n/4 + \gamma_n, \quad \lim_{n\to\infty} \gamma_n = 7/4.$$

Concerning to the problem of approximation to p-adic numbers by algebraic numbers there is only one paper of J. Morrison (1978), which contains the direct p-adic analogue of Wirsing's theorem:

$$A = n/2 + 3/2.$$

This result was slightly refined in this year:

$$A = n/2 + \gamma_n, \quad \lim_{n\to\infty} \gamma_n = 3/2.$$

Finally, I want to say some words about one more interesting subject, namely about a simultaneous case. It was natural to make the following

CONJECTURE. *For any two real numbers $\xi_1, \ \xi_2$ which are not algebraic numbers of degree $\leq n$, there exist infinitely many algebraic numbers $\alpha_1, \ \alpha_2$ such that*

$$\begin{cases} |\xi_1 - \alpha_1| \ll \boxed{P}^{-(n+1)/2}, \\ |\xi_2 - \alpha_2| \ll \boxed{P}^{-(n+1)/2}, \end{cases}$$

where $P(x) \in \mathbb{Z}[x], \ \ P(\alpha_1) = P(\alpha_2) = 0, \deg P \leq n$. The implicit constant in $\ll$ should depend on $\xi_1, \ \xi_2$, and n.

Using Sprindžuk's method one can prove it for almost all real numbers. However, this is not true for all real numbers. In 2001 D. Roy and M. Waldschmidt constructed the following

COUNTER-EXAMPLE (ROY-WALDSCHMIDT, 2001). *For any sufficiently large n there exist real numbers ξ_1 and ξ_2 such that*

$$\max\{|\xi_1 - \alpha_1|, |\xi_2 - \alpha_2|\} > \boxed{P}^{-\sqrt{n}}.$$

At the same time we can prove the following

THEOREM. *Let $\xi_1, \ \xi_2$ be real numbers which are not algebraic numbers of degree $\leq n$. Then at least one of the following assertions is true:*

(i) There exist infinitely many algebraic numbers $\alpha_1, \ \alpha_2$ such that

$$\begin{cases} |\xi_1 - \alpha_1| \ll \boxed{P}^{-A_1-1}, \\ |\xi_2 - \alpha_2| \ll \boxed{P}^{-A_1-1}. \end{cases}$$

where $0 < A_1 < n/4 - 1/2$;

(ii) For some $\xi \in \{\xi_1,\ \xi_2\}$ *there exist infinitely many algebraic numbers* α *of degree* $2 \leq k \leq [2A_1] + 1$ *such that*

$$|\xi - \alpha| \ll H(\alpha)^{-A_2},$$

where

$$A_2 = \frac{A_1(n - 2k + 6) + n - 4k + 6}{2(2A_1 - k + 2)}.$$

The implicit constants in $\ll$ *depend on* $\xi_1,\ \xi_2,$ *and* n.