Hilbert's Irreducibility Theorem

Navid SAFAEI, Radosław ŻAK***

*Head of Mathematical Olympiad department, Salam Schools Complex, Tehran, Iran Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia
**PhD student, University of Oxford

Number theory is among fields of mathematics which use methods from other areas the most. One incoming stream of tools comes from mathematical analysis. Over the past years analytical number theory got increasingly popular even in the context of mathematical olympiads; Tomek Kobos's article in Δ^3_{16} showcases a nice selection of common methods. However, the 'alien' concepts of limits, series, convergence and derivatives might be slightly intimidating for students new to this area. One of advantages of Hilbert's Irreducibility Theorem (HIT for short) is that it packs a lot of insight from analysis and/or algebraic geometry in an understandable, number theoretical form.

Recall that *a polynomial in two variables* $P(x, y)$ is a finite sum of monomials, each of which has a form $a_{ij}x^iy^j$. We will mostly work in the case when numbers a_{ij} are integers; the set of all such polynomials will be denoted by $\mathbb{Z}[x, y]$. Among examples we can list $x^3 - y^2$, $x^2 - 2xy + 2y^2$ or $x^3 - x^2y + y^4 + 1$. Another example is $y^3 - 2y + 1$, although it doesn't contain the variable x, and we might want to be careful about that. We have the corresponding notion of the degree for two-variable polynomials – by definition, the degree of monomial $a_{ij}x^iy^j$ is $i + j$, and the *degree of a polynomial* is the maximum of degrees of its monomials. We can also define the *degree in a particular variable*; the degree of $P(x, y)$ in x is just the usual degree if we forget about the fact that y is a variable. For instance, the polynomial $P(x, y) = x^3 - x^2y^3 + y^4 + 2$ has

$$\deg P(x, y) = 5, \quad \deg_x P(x, y) = 3, \quad \deg_y P(x, y) = 4.$$

Similarly as in one-variable case, we say $P(x, y)$ is *reducible* if it can be written as a product $P_1(x, y)P_2(x, y)$ where P_1, P_2 are non-constant polynomials; otherwise we say it's *irreducible*. A well-known tool called Gauss' Lemma implies that if $P(x, y)$ has integer coefficients and it decomposes as $P_1(x, y) \cdot P_2(x, y)$, where P_1, P_2 have **rational** coefficients, then we can also find such an example of P_1, P_2 with **integer** coefficients.

As with primes and integers, irreducible polynomials can be thought of as building blocks: any polynomial $P(x, y)$ can be written as a product $Q_1(x, y)^{\alpha_1} \cdot \ldots \cdot Q_k(x, y)^{\alpha_k}$, for some irreducible polynomials $Q_1, \ldots, Q_k$ and some positive integer exponents α_i.

A curious reader can find the proof of HIT in:

M. Villarino, W. Gasarch, K. Regan, *Hilbert's Proof of His Irreducibility Theorem*, Amer. Math. Monthly (2018), doi.org/10.1080/00029890.2018.1448181, arXiv:1611.06303

Theorem 1 (Hilbert)**.** Let $P(x, y)$ be an irreducible polynomial with integer coefficients, which is dependent on the variable x (i.e., $\deg_x P(x, y) > 0$). Then we can find infinitely many integers t for which the (one-variable) polynomial $f_t(y) := P(t, y)$ is also irreducible, and moreover $\deg f_t = \deg_y P(t, y)$.

An easy example: $Q(x, y) = y^2 - x$ is irreducible. If we try to put $t = 1$, then the polynomial $Q(1, y) = y^2 - 1$ factors as $(y - 1)(y + 1)$. However it's not hard to see that such factorisation occurs precisely when t is a square – thus, we can choose any t which is not a square, and obtain an irreducible polynomial. We can go even further.

Proposition 2. Suppose $R(x)$ is a polynomial with integer coefficients such that $R(t)$ is a square for any integer t. Then there is a polynomial $Q(x)$ with integer coefficients such that $R(x) = Q(x)^2$.

Proof. Consider the polynomial $P(x, y) = y^2 - R(x)$. Suppose it is irreducible. Then by HIT we can find an integer t such that $P(t, y)$ is irreducible. But we know $R(t) = a^2$ for some a, and so $P(t, y) = y^2 - a^2 = (y - a)(y + a)$ is reducible. This contradiction means that $P(x, y)$ is reducible.

Therefore we can find P_1, P_2 with integer coefficients, non-constant, so that $P(x, y) = P_1(x, y)P_2(x, y)$. If $\deg_y P_1 = 0$ (so P_1 doesn't contain y), then P_1 would depend only on x, and it would have to divide the leading coefficient of y in $P(x, y)$. But this is 1, so this is impossible. Hence the only possible case is that

both P_1 and P_2 are linear in y (as $\deg_y P(x,y) = 2$). But then by examining leading coefficients again, we get that $P_1(x,y) = y + Q_1(x)$, $P_2(x) = y + Q_2(x)$ for some polynomials Q_1, Q_2 (as those leading coefficients multiply to 1, and we can multiply our polynomials by -1 if needed, without loss of generality). Therefore

$$\begin{aligned} y^2 - R(x) = P(x,y) &= P_1(x,y)P_2(x,y) = (y + Q_1(x))(y + Q_2(x)) \\ &= y^2 + y(Q_1(x) + Q_2(x)) + Q_1(x)Q_2(x). \end{aligned}$$

By comparing coefficients, we get $Q_1(x) + Q_2(x) = 0$, and so $R(x) = -Q_1(x)Q_2(x) = Q_1(x)^2$. □

In fact, we can prove something even stronger. We will have to use the following, innocently-looking fact. However, we remark this is not easy to prove; one of its proofs involves Chebotarev's theorem.

Theorem 3. If $f(x)$ is an irreducible polynomial with integer coefficients with $\deg f \geqslant 2$, then there are infinitely many primes p which do not divide $f(t)$ for any integer t.

Our final goal is to prove the following:

More on Theorem 4 can be found here:
H. Davenport, D. Lewis, A. Schinzel, *Polynomials of certain special types*, Acta Arith. (1964),
http://eudml.org/doc/207456

Theorem 4. Let $P(x,y) \in \mathbb{Z}[x,y]$ be a polynomial with the following property: for any non-constant arithmetic sequence $(a_n)_{n=-\infty}^{\infty}$ of integers, we can find an index $i \in \mathbb{Z}$ and an integer y such that $P(a_i, y) = 0$. Then there is a polynomial $R(x) \in \mathbb{Q}[x]$ such that $P(x, R(x)) = 0$ identically.

This will generalise our previous Proposition 2 in two ways. First, we no longer need every t to satisfy something, but only sufficiently many such t's to cover all integer arithmetic sequences. Second, we could be using any polynomial in place of y^2. A problem at the end of this article illustrates this last observation.

Proof of Theorem 4. First observe that our condition on arithmetic sequences actually gives us infinitely many indices i for which $P(a_i, y) = 0$ has a solution in y. Indeed, we know there is at least one such i, but then $a'_j := a_{i+1+2j}$ is also an arithmetic sequence (these are odd terms of (a_n) if i is even, and even terms if i is odd), which is a subset of (a_n) not containing a_i. This way we get another index, and we can continue this process as long as we want.

We can factor $P(x,y)$ as a product $Q_1(x,y) \cdot \ldots \cdot Q_k(x,y)$, for some irreducible polynomials Q_j (not necessarily distinct). If any Q_j depends only on x, then we can safely ignore this component, as it only gives us finitely many t's for which $P(t,y) = 0$ has a solution. Similarly if $Q_j(x,y) = 0$ itself has only finitely many solutions in x and y, we can ignore it – indeed, in both cases the polynomial $P' := P/Q_j$ satisfies both the problem's assumptions and its claim if and only if P does.

We can now use HIT to find numbers t_j such that each $Q_j(t_j, y)$ is an irreducible polynomial, with the same degree in y as $Q_j(x,y)$ originally was. If this degree is at least 2 for every j, then we can use Theorem 3 to obtain primes p_j so that $p_j \nmid Q_j(t_j, y)$, for each j; moreover we can choose these primes to be pairwise distinct.

Now let's use Chinese Remainder Theorem to find a solution to the system of congruences $t \equiv t_j \pmod{p_j}$ for $j = 1, \ldots, k$. The solution will be of form $t \equiv c \pmod{p_1 p_2 \ldots p_k}$ for some c. In other words, the set of solutions forms the arithmetic sequence $a_i = c + i p_1 p_2 \ldots p_k$. We know we will find i and y such that $P(a_i, y) = 0$. Therefore, $Q_j(a_i, y) = 0$ for some j. But at the same time

$$Q_j(a_i, y) \equiv Q_j(t_j, y) \not\equiv 0 \pmod{p_j},$$

and so we get a contradiction.

Hence some Q_j is linear in y; without loss of generality it's Q_1. We can write $Q_1(x,y) = A(x)y + B(x)$ for A, B polynomials. We already commented why we can assume that each $Q_j(x,y) = 0$ has infinitely many solutions in (x,y); therefore $A(x)$ divides $B(x)$ for infinitely many values of x. But this means that

$A(x)$ divides $B(x)$ as a polynomial (for that, consider $\gcd(A(x), B(x))$). Therefore $R(x) = -\frac{B(x)}{A(x)}$ is a polynomial, and hence $P(x, R(x)) = Q_1(x, R(x)) = 0$. □

A careful reader will notice that Theorem 4 only gives R with rational, and not integer, coefficients. Indeed, if we took $P(x, y) = x^2 + x - 2y$, we would get $R(x) = \frac{x(x+1)}{2}$. We finish by presenting a problem illustrating that in some situations we can actually get $R(x)$ to have integer coefficients.

Problem. Suppose P, Q are two polynomials with integer coefficients, such that for any integer n we can find an integer m so that $P(n) = Q(m)$. Prove that then there is a polynomial $R(x)$ with rational coefficients such that $P(x) = Q(R(x))$. Moreover, if polynomial $Q(\frac{x}{k})$ does not have integer coefficients for any $k \geqslant 2$, prove that $R(x)$ has integer coefficients.

Can the policemen catch the thief?

*Alexandru BENESCU**

*Student, Tudor Vianu National College of Computer Science, Romania

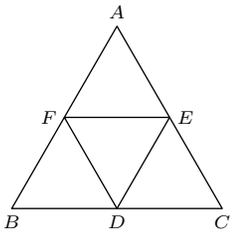

Fig. 1

In this article, we will address the following problem.

In a village there is a thief and n policemen. The alleys in this village form an equilateral triangle along with its midlines (Fig. 1). The thief's maximum speed is $\kappa > 0$ times greater than the policemen's maximum speed. Given that everyone can see each other and the (continuous) movement is possible only along the alleys, determine whether the policemen can catch the thief from any starting position?

Let us start the solution by analysing some simple cases. Assume that there is only one policeman, i.e. $n = 1$. This situation is trivial. If $\kappa < 1$ (i.e., the thief is slower than the policeman), the policeman has a winning strategy: he can chase the thief regardless of the route the latter takes, eventually catching him. If $\kappa \geqslant 1$, the thief has a winning strategy by looping in a cycle (such as $A \to B \to C \to A$ in Fig. 1) and adjusting his velocity and direction according to the policeman's movement.

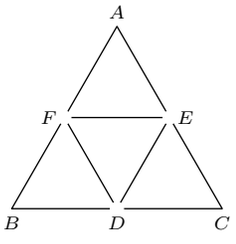

Fig. 2

The situation changes drastically (in favour of justice) if there are three (or more) policemen. We prove that in this case they will catch the thief regardless of his speed. One possible strategy for them is to position themselves at points D, E and F, respectively (using the notation of Fig. 1). In this way they partition the whole village into six connected parts (or components), as shown in Fig. 2. One of these parts contains the thief, and this part (like every other one) is closed at both ends by policemen. It is enough for one of them to move towards the other, thus catching the thief.

It remains to consider the case of two policemen, which is more demanding. First, we prove that for $\kappa \leqslant 3$ the police win. The first policeman is the one to chase the thief (that is why we'll call him *the chaser*). His only task is to prevent the thief from hiding forever in one place. More precisely, he has to make sure that the thief's *last-visited middle node* keeps changing over time (by *middle node* we mean D, E, or F). It is easy to see that only one policeman is enough to ensure this.

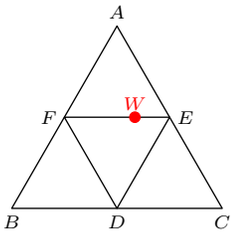

Fig. 3

The second policeman, whom we'll call *the watcher*), has a more subtle task. Firstly he needs to go to point W that splits the segment EF in a $1:2$ ratio (Fig. 3); he does not need to hurry. When he gets there he needs to watch the thief closely (as watchers do). Basically his task is to cut off the thief's escape route whenever possible. For example, if the thief enters the 'upper corner' $E-A-F$ through point E, the watcher must prevent the thief from escaping this corner through point F. It is possible to do so since $\frac{|EA|+|AF|}{|WF|} = 3 \geqslant \kappa$. There is also one tiny catch – at the same time the thief comes back to the point E, the watcher needs to be back at point W. But this can be ensured