On the representation of primes by polynomials (a survey of some recent results)

B.Z. Moroz

0. This survey article has appeared in: Proceedings of the Mathematical Institute of the Belarussian Academy of Sciences, 13 (2005), no. 1, pp. 114-119. Multiplying it as an MPIM preprint, I should mention a new book, in which some of the problems, mentioned in my paper, are discussed in detail: G. Harman, Prime-detecting sieves, LMS Monographs series 33, Princeton University Press, Princeton, NJ, 2007.

1. About seven years ago J. Friedlander and H. Iwaniec [3] - [5] proved that there are infinitely many primes of the form $x^2 + y^4$. Inspired by their work, but by a different method, D.R. Heath-Brown [7] shows that the binary cubic form $x^3 + 2y^3$ represents infinitely many prime numbers, thereby confirming the conjecture of G.H. Hardy and J.E. Littlewood on the infinity of primes expressible as a sum of three cubes. Subsequently, it has been shown [8] that any irreducble primitive binary cubic form with integral rational coefficients takes infinitely many prime values if it takes at least one odd value. Indeed, we prove [9] an analogous theorem even for certain binary non-homogeneuos cubic polynomials. I intend to briefly describe the background of the problem, to formulate the main theorems proved in the works [4], [5], [7] - [9], and to survey some of the ideas leading to the proof of those results.

Notation. As usual, $\mathbb{Q}, \mathbb{Z}$, and $\mathbb{N}$ stand for the field of rational numbers, the ring of rational integers, and the set of positive rational integers respectively; let $P = \{\pm 2, \pm 3, \pm 5, \dots\}$ be the set of the rational primes. Let $\#\, S$ stand for the cardinality of a set S; given a subset S of $\mathbb{Z}$, let h.c.f.(S) denote the highest common factor of the elements of S.

In 1854, V. Ya. Bouniakowsky proposed the following conjecture (cf. [1, p. 33]).

Conjecture 1. *Let $f(t) \in \mathbb{Z}[t]$ and suppose that the polynomial $f(t)$ is irreducible in $\mathbb{Q}[t]$ and that* h.c.f.$(\{f(a) : a \in \mathbb{Z}\}) = 1$. *Then the set*

$$\{f(a) : a \in \mathbb{Z}\} \cap P$$

is infinite.

So far Conjecture 1 has been settled only for linear polynomials (*L.G. Dirichlet*, 1837; cf. [1, p. 415]). The following conjecture is an easy consequence of Conjecture 1 (cf. [14, Lemma 4 on p. 33]).

Conjecture 2. *Let* $f(\vec{x}) \in \mathbb{Z}[\vec{x}]$, $\vec{x} := (x_1, \dots, x_n)$, *and suppose that the polynomial* $f(\vec{x})$ *is irreducible in* $\mathbb{Q}[\vec{x}]$ *and that* h.c.f.$(\{f(\vec{a}) : \vec{a} \in \mathbb{Z}^n\}) = 1$. *Then the set*

$$\{f(\vec{a}) : \vec{a} \in \mathbb{Z}^n\} \cap P$$

is infinite.

On the other hand, in 1970 Yu.V. Matiyasevich [12] proved the following theorem.

Theorem 1. *For any listable subset* $\mathcal{A}$ *of* $\mathbb{N}$, *there is a polynomial* $Q_{\mathcal{A}}(\vec{x})$ *in* $\mathbb{Z}[\vec{x}]$ *such that*

$$\{Q_{\mathcal{A}}(\vec{a}) : \vec{a} \in \mathbb{Z}^n\} \cap \mathbb{N} = \mathcal{A}.$$

Corollary 1. *There are polynomials* $Q_1(\vec{x})$ *and* $Q_2(\vec{x})$ *in* $\mathbb{Z}[\vec{x}]$ *such that*

$$\{Q_1(\vec{a}) : \vec{a} \in \mathbb{Z}^n\} \cap \mathbb{N} = P \cap \mathbb{N}$$

and

$$\{Q_2(\vec{a}) : \vec{a} \in \mathbb{Z}^n\} \cap \mathbb{N} = \mathbb{N} \setminus P.$$

Proof. Since both $P \cap \mathbb{N}$ and $\mathbb{N} \setminus P$ are listable sets, the assertion follows from Theorem 1.

Corollary 1 shows that the set P can not be replaced by the set $P \cap \mathbb{N}$ of positive primes in Conjecture 2, although Conjecture 1 can be, of course, re-stated as follows.

Conjecture 1a. *Let* $f(t) \in \mathbb{Z}[t]$; *suppose that the polynomial* $f(t)$ *is irreducible in* $\mathbb{Q}[t]$, *that* h.c.f.$(\{f(a) : a \in \mathbb{Z}\}) = 1$, *and that* $f(a) \to \infty$ *as* $a \to \infty$. *Then the set*

$$\{f(a) : a \in \mathbb{Z}\} \cap P \cap \mathbb{N}$$

is infinite.

In 1840, L.G. Dirichlet proved Conjecture 2 for binary quadratic forms (cf. [1, p. 417]). H. Iwaniec [11] extended Dirichlet's result to quadratic polynomials in two variables.

Let us cite a few lines from Heath-Brown's work [7]: "In measuring the quality of any theorem on the representation of primes by integer polynomial $f(x_1, \ldots, x_n)$ in several variables, it is useful to consider the exponent $\alpha(f)$, defined as follows. Let $|f|$ denote the polynomial obtained by replacing each coefficient of f by its absolute value, and define $\alpha(f)$ to be the infimum of those real numbers α for which

$$\# \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : |f|(x_1, \ldots, x_n) \leq X\} \leq X^\alpha.$$

Thus $\alpha(f)$ measures the frequency of values taken by f. If $\alpha(f) \geq 1$ we expect f to represent at least $X^{1-\epsilon}$ of the integers up to X, while if $\alpha(f) < 1$ we expect around X^α such integers to be representable. Thus the smaller the value of $\alpha(f)$, the harder it will be to to prove that f represents primes."

The two classical theorems of L.G. Dirichlet mentioned above, as well as the theorem of H. Iwaniec [11], all correspond to the value $\alpha(f) = 1$. Conjecture 2 had been proved for **no** polynomial f with $\alpha(f) < 1$ prior to the work of J. Friedlander and H. Iwaniec [3] - [5]. It is clear that $\alpha(f) = \frac{3}{4}$ for the polynomial $f(x_1, x_2) = x_1^2 + x_2^4$ of Friedlander and Iwaniec and that $\alpha(f) = \frac{2}{3}$ if $f(x_1, x_2)$ is a binary cubic form. For the simplest non-linear polynomial $f(x) = x^2 + 1$ of one variable, $\alpha(f) = \frac{1}{2}$.

2. Let us now state the recent results alluded to in n^o 1.

Theorem 2 (see [4]). *Conjecture 2 holds true for the polynomial*

$$f(x_1, x_2) = x_1^2 + x_2^4.$$

Specifically,

$$\sum_{\vec{a} \in \mathbb{N}^2,\ f(\vec{a}) \leq X} \Lambda(f(\vec{a})) = \frac{4}{\pi} \kappa X^{\frac{3}{4}} (1 + O(\frac{\log \log X}{\log X}))$$

as $X \to \infty$, *where* Λ *is the* **von Mangoldt** *function and*

$$\kappa := \int_0^1 (1 - t^4)^{1/2} = \Gamma(\frac{1}{4})^2 / 6\sqrt{2\pi}.$$

Theorem 3 (see [7]). *Conjecture 2 holds true for the polynomial*

$$f(x_1, x_2) = x_1^3 + 2x_2^3 .$$

Specifically, there is a positive constant c *such that, if* $\eta = \eta(X) = (\log X)^{-c}$, *then the number of primes of the form* $a^3 + 2b^3$ *with integer* a, b *in the interval* $X < a, b \leq X(1 + \eta)$ *is equal to*

$$\sigma_0 \, \frac{\eta^2 X^2}{3 \log X} \, \{1 + O((\log \log X)^{-1/6})\}$$

as $X \to \infty$, *where*

$$\sigma_0 := \prod_{p \in P \cap \mathbb{N}} (1 - \frac{\nu_p - 1}{p})$$

and ν_p *stands for the number of solutions of the congruence* $x^3 \equiv 2 \mod p$.

Theorem 4 (see [8]). *Let* $f(\vec{x})$ *be a primitive binary cubic form with integral rational coefficients irreducible in* $\mathbb{Z}[\vec{x}]$. *There are infinitely many primes of the form* $f(\vec{a})$ *with* $\vec{a} \in \mathbb{Z}^2$ *unless* $f(\vec{a})$ *is divisible by 2 for each* $\vec{a}$ *in* $\mathbb{Z}^2$, *in which case there are infinitely many primes of the form* $\frac{1}{2} f(\vec{a})$ *with* $\vec{a} \in \mathbb{Z}^2$.

Theorem 5 (see [9]). *Let* $f_0(\vec{x})$ *be a binary cubic form with integral rational coefficients irreducible in* $\mathbb{Z}[\vec{x}]$. *For* $d \in \mathbb{Z}$ *and* $\vec{\gamma} \in \mathbb{Z}^2$, *let the positive integer* γ_0 *be chosen so that* $f(\vec{x}) = \gamma_0^{-1} f_0(\vec{\gamma} + d\vec{x})$ *is a primitive polynomial with integral rational coefficients. Suppose, moreover, that*

$$\text{h.c.f.}(\{f(\vec{a}) : \vec{a} \in \mathbb{Z}^n\}) = 1.$$

Then the set $f(\mathbb{Z}^2)$ *contains infinitely many rational primes.*

Remark 1. One can actually obtain an asymptotic formula for the relevant number of primes in Theorems 4 and 5, of the same shape as in Theorem 3.

The statement of Theorem 5 has been used, as an unproved hypothesis, in Heath-Brown's work [6] on rational solubility of diagonal cubic equations in five variables. We can now establish these results unconditionally, as a corollary to Theorem 5 (see [9, Corollary 1.1] and [6] for the details).

Corollary 2. *Let* H *be the hypersurface defined by the equation*

$$\sum_{i=1}^{5} a_i x_i^3 = 0$$

with $a_i \in \mathbb{Z}$ *for* $1 \leq i \leq 5$. *Suppose that the integers* a_i, $1 \leq i \leq 5$, *are divisible neither by 3, nor by* p^2 *for* $p \in P$, $p \equiv 2 \mod 3$. *Then the hypersurface* H *satisfies the Hasse principle, providing that the Selmer Parity Conjecture holds for the class of elliptic curves given by the equations*

$$x^3 + y^3 = A$$

with $A \in \mathbb{Z}/\{0, 1\}$.

The next corollary follows from the work of P. Satgé [13] and Theorem 5; cf. [9, Corollary 1.2].

Corollary 3. *Let a and b be coprime rational integers satisfying one of the following congruence conditions:*

$$a \pm b \equiv 0 \pmod 9 \text{ or } \{\bar{a}, \bar{b}\} \cap \{\pm 2, \pm 3\} \neq \emptyset,$$

where $\bar{c}$ stands for the residue of the integer c modulo 9. Then the equation

$$x_1^3 + 2x_2^3 + ax_3^3 + bx_4^3 = 0$$

has infinitely many solutions (x_1, x_2, x_3, x_4) in $\mathbb{Z}^4$ with

$$\text{h.c.f.}(x_1, x_2, x_3, x_4) = 1.$$

3. Theorems 2 - 5 are proved by sieve methods. Given a sequence

$$\mathcal{A} = (a_n)_{n \in N}$$

of non-negative integers, one should like to evaluate asymptotically the sum

$$\sum_{p \in P \cap \mathbb{N},\, p \leq x} a_p$$

or, as in Theorem 2, the sum

$$S(x) := \sum_{n \leq x} a_n \Lambda(n).$$

Let

$$A(x) := \sum_{n \leq x} a_n;$$

it follows that

$$S(x) = -\sum_{d \leq x} (\mu(d) \log d) A_d(x),$$

where

$$A_d(x) := \sum_{n \leq x,\, d | n} a_n.$$

J. Friedlander and H. Iwaniec [5] introduce the following assumptions:

$$A(x) \gg A(\sqrt{x})(\log x)^2,\ A(x) \gg x^{1/3} (\sum_{n \leq x} a_n^2)^{1/2}; \tag{1}$$

$$A_d(x) = g(d)A(x) + r_d(x), \tag{2}$$

where g is a multiplicative function such that

$$\begin{aligned} 0 \le g(p^2) \le g(p) &< 1,\ g(p) \gg p^{-1},\ g(p^2) \gg p^{-2},\ \text{for } p \in P \cap \mathbb{N},\ \text{and} \\ \sum_{p \in P \cap \mathbb{N},\ p \le x} g(p) &= \log\log y + c_0(g) + O((\log y)^{-c_1}); \end{aligned} \tag{3}$$

$$A_d(x) \ll \frac{\tau(d)^{c_2}}{d} A(x) \tag{4}$$

uniformly in the range $1 \le d \le x^{1/3}$;

$$\sum_{d \le D(x)(\log x)^{c_2}} \mu_3(d)|r_d(t)| \le A(x)(\log x)^{-c_3} \tag{5}$$

for $t \le x$ and some $D(x)$ in the range $x^{2/3} < D(x) < x$, where $\mu_3(d)$ stands for the characteristic function of the cube-free integers and $\tau(d)$ denotes the number of divisors of d in $\mathbb{N}$.

Assumptions (1) - (5), or their analogues, belong to the standard theory of sieve methods. It is well-known that those assumptions alone do not suffice to obtain the desired asymptotic formulae, or even lower bounds, for the sums $A(x)$ or $S(x)$ because of the following *"parity phenomenon"* (cf. [15]). Let a_n be the characteristic function of the set of those positive integers, which are composed of an even number of prime factors, then the sequence $\mathcal{A} = (a_n)_{n \in N}$ satisfies conditions (1) - (5) but $a_p = 0$ for $p \in P \cap \mathbb{N}$.

The crucial new assumption made in the works [3] - [5] is as follows:

$$\sum_{m \le x} \Big| \sum_{\substack{N < n \le 2N,\ mn \le x \\ \text{h.c.f.}(n, m\Pi) = 1}} \beta(n, C)\, a_{mn} \Big| \le A(x)(\log x)^{-c_4} \tag{6}$$

for every N in the range

$$\frac{\sqrt{D(x)}}{\Delta(x)} < N < \frac{\sqrt{x}}{\delta(x)}$$

and every C in the range

$$1 \le C \le \frac{x}{D(x)},$$

where $\Delta(x) \ge \delta(x) \ge 2$,

$$\beta(n, C) = \mu(n) \sum_{d | n,\ d \le C} \mu(d),$$

and Π is equal to the product of the positive primes up to some p_0, satisfying the inequalities

$$2 \leq p_0 \leq \Delta(x)^{1/c_5 \log\log x}.$$

Here $c_i,\ 1 \leq i \leq 5$, are suitable positive numerical constants.

Theorem 6 (see [5]). *Assume (1) - (6). Then the following asymptotic formula holds true:*

$$\sum_{p \in P \cap \mathbb{N},\, p \leq x} a_p \log p = HA(x)(1 + O(\frac{\log \delta(x)}{\log \Delta(x)}))$$

with

$$H := \prod_{p \in P \cap \mathbb{N}} (1 - g(p))(1 - \frac{1}{p})^{-1},$$

where the implied O-constant depends at most on g.

It is not too difficult to verify the assumptions (1) - (4) for the sequence

$$a_n := \#\ \{(b_1, b_2) \in \mathbb{N}^2 : b_1^2 + b_2^4 = n\}$$

studied in [3] - [5]. Assumption (5) has been established for that sequence by E. Fouvry and H. Iwaniec [2]. The main difficulty lies in proving the estimate (6) for the bilinear forms; the authors' strategy depends on the subtle analysis in the spirit of Hecke's "multidimensional arithmetic" [10] for the Gaussian field $\mathbb{Q}(\sqrt{-1})$, as it has been explained in the Introduction to the work [4] and in the note [3].

The sieve procedure, set up by Heath-Brown [7] to prove Theorem 3 and used in our works [8] and [9] to prove Theorems 4 and 5, has much in common with the approach of Friedlander and Iwaniec in [3] - [5], although their assumption (5) does not hold for the sequences

$$a_n := \#\ \{\vec{b} \in \mathbb{N}^2 : f(\vec{b}) = n\}$$

in Theorems 3 - 5. The main novelty, introduced in the work [7] and further developed in the works [8] and [9], is the "Type II" bound which goes beyond the standard assumptions (1) - (5) of the classical sieve theory, as does the estimate (6) in the works [3] - [5].

Let k be a cubic number field, that is an extension of $\mathbb{Q}$ with $[k : \mathbb{Q}] = 3$, and let $\mathfrak{o}$ be the ring of integers of k. Let $\{\omega_1,\ \omega_2\} \subset \mathfrak{o}$, suppose that $\omega_2 \neq 0,\ \omega_1/\omega_2 \notin \mathbb{Q}$, and let

$$\mathcal{A} := \{(a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1} :\ (a_1, a_2) \in \mathbb{Z}^2,\ X < a_1, a_2 \leq X(1 + \eta),$$

$$\text{h.c.f.}(a_1, a_2) = 1\},$$

where $\mathfrak{d}$ stands for the ideal in $\mathfrak{o}$, generated by ω_1 and ω_2. Proving Theorem 4 amounts to estimating the number of prime ideals in $\mathcal{A}$. The "Type II" bound is an upper estimate for the sums of the following form:

$$\sum_{\substack{\mathfrak{ab}\in\mathcal{A} \\ V<N\mathfrak{b}\leq 2V}} b_{\mathfrak{a}} g_{\mathfrak{b}}$$

with V ranging over the interval

$$X^{1+\tau} \ll V \ll X^{3/2-\tau}, \ \tau := (\log\log X)^{-1/6},$$

where the function $\mathfrak{a} \mapsto b_{\mathfrak{a}}$ takes its values in the set $\{0, 1\}$ and $\mathfrak{b} \mapsto g_{\mathfrak{b}}$ is a real-valued function. To estimate those sums one makes use of Hecke's three-dimensional arithmetic of a cubic number field; cf. [7] - [9].

Acknowledgement. It is a pleasure to thank Professor V.I. Bernik for inviting me to attend the conference "Diophantine analysis, uniform distributions, and applications" in Minsk and for his kind hospitality during my visit. I am indebted to Professor A. Schinzel for the reference [14].

References

[1] L.E. Dickson, *History of the theory of numbers,* vol. 1, Chelsea Publ. Company, New York, 1952.

[2] E. Fouvry and H. Iwaniec, Gaussian primes, *Acta Arithmetica*, 79 (1997), 249-387.

[3] J. Friedlander and H. Iwaniec, Using a parity-sensitive sieve to count prime values of a polynomial, *Proceedings of the National Academy of Sciences of the USA* 94 (1997), 1054-1058.

[4] J. Friedlander and H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Annals of Mathematics,* 148 (1998), 945-1040.

[5] J. Friedlander and H. Iwaniec, Asymptotic sieve for primes, *Annals of Mathematics,* 148 (1998), 1041-1065.

[6] D.R. Heath-Brown, The solubility of diagonal cubic Diophantine equations, *Proceedings of the London Mathematical Society (3),* 79 (1999), 241-259.

[7] D.R. Heath-Brown, Primes represented by $x^3 + 2y^3$, *Acta Mathematica,* 186 (2001), 1-84.

[8] D.R. Heath-Brown and B.Z. Moroz, Primes represented by binary cubic forms, *Proceedings of the London Mathematical Society (3),* 84 (2002), 257-288.

[9] D.R. Heath-Brown and B.Z. Moroz, On the representation of primes by cubic polynomials in two variables, *Proceedings of the London Mathematical Society (3),* 88 (2004), 289-312.

[10] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, *Mathematische Zeitschrift,* 6 (1920), 11-51.

[11] H. Iwaniec, Primes represented by quadratic polynomials in two variables, *Acta Arithmetica*, 24 (1974), 435-322.

[12] Yu.V. Matiyasevich, On the relation between two conjectures on polynomials, *Doklady Akademii Nauk SSSR (ser. matemat.)*, 191 (1970), 279-282.

[13] P. Satgé, Un analogue du calcul de Heegner, *Invent. Math.,* 87 (1987), 425-439.

[14] A. Schinzel, On the relation between two conjectures on polynomials, *Acta Arithmetica*, 38 (1981), 285-322.

[15] A. Selberg, On elementary methods in prime number theory, *Collected papers,* vol. 1, pp. 425-439, Springer-Verlag, 1989.

Author's address:

B.Z. Moroz,
Max-Planck-Institut für Mathematik,
Vivatgasse 7, D-53111 Bonn, Germany

E-mail address: moroz@mpim-bonn.mpg.de