Quadratic forms with polynomial coefficients

by

MIREILLE CAR (Marseille)

Introduction. If x is a strictly positive real number let H(x) denote the number of pairs (a, b), $a, b \in \mathbb{Z}$, such that $|a| \leq x$, $|b| \leq x$ and such that the ternary quadratic form $X^2 + aY^2 + bZ^2$ represents 0 over the field \mathbb{Q} of rational numbers. Similarly, let N(x) denote the number of 3-tuples $(a, b, c) \in \mathbb{Z}^3$ such that $|a| \leq x$, $|b| \leq x$, $|c| \leq x$, and such that the ternary quadratic form $aX^2 + bY^2 + cZ^2$ represents 0 over the field \mathbb{Q} . In [6] Serre proved that

$$H(x) \ll \frac{x^2}{\log x}$$
 and $N(x) \ll \frac{x^3}{(\log x)^{3/2}}$,

and asked if

$$H(x) \gg \frac{x^2}{\log x}$$
 and $N(x) \gg \frac{x^3}{(\log x)^{3/2}}$.

Using Burgess's estimate for character sums and sieve methods, C. Hooley [4] proved that

$$N(x) \gg \frac{x^3}{(\log x)^{3/2}}$$

Guo [1] improved Hooley's result, giving an asymptotic estimate for the number $N_1(x)$ of ternary quadratic forms $aX^2 + bY^2 + cZ^2$ which represent zero over \mathbb{Q} and whose coefficients a, b, c are square-free rational integers, pairwise coprime and such that $|a| \leq x, |b| \leq x, |c| \leq x$, and mentioned that the expected lower bound for H(x) is an immediate corollary. He proved that for x tending to ∞ ,

$$N_1(x) = \frac{9/7}{\Gamma(3/2)^2} \left\{ \prod_p \left(1 - \frac{1}{p} \right)^{3/2} \left(1 + \frac{3}{2p} \right) \right\} \frac{x^3}{(\log x)^{3/2}} + O\left(\frac{x^3}{(\log x)^2} \right),$$

the product being over the rational primes.

2000 Mathematics Subject Classification: 11T06, 11T55.

Key words and phrases: polynomials, finite fields, quadratic forms.

M. Car

In what follows, we prove analogous results, with \mathbb{Z} replaced by the ring $\mathbb{F}_q[T]$, where \mathbb{F}_q is a finite field with q elements and odd characteristic. J.-P. Serre suggested this problem to the author who wants to thank him for that and for all his useful remarks. For the precise statement of the results, see Section 1. For example, a simple one is the following.

THEOREM. For n > 0, let Q(n) denote the number of pairs (A, B) of polynomials $A \in \mathbb{F}_q[T]$, $B \in \mathbb{F}_q[T]$ such that deg $A = \deg B = n$ and such that the ternary quadratic form $X^2 - AY^2 - BZ^2$ represents 0 over the field $\mathbb{F}_q(T)$. Then, for any even integer n > 0,

$$Q(n) = \frac{2q(q-1)}{\pi} C(q) \frac{q^{2n}}{n} + O\left(\frac{q^{2n}}{n^2}\right),$$

and for any odd integer n > 0,

$$Q(n) = \frac{q(q-1)}{\pi} C(q) \frac{q^{2n}}{n} + O\left(\frac{q^{2n}}{n^2}\right),$$

with

$$C(q) = \prod_{P} \left(1 + \frac{1}{2q^{\deg P}(q^{\deg P} + 1)} \right),$$

the product being over the monic irreducible polynomials, with the constants involved in the O symbol depending only on q.

Thus, q^n acts as x in the rational case, and n acts as $\log x$ in the rational case.

1. Notations and statement of the results. Let us fix some notation. Let q be a power of an odd prime number and let \mathbb{F}_q denote the finite field with q elements. Let $\mathbb{A} = \mathbb{F}_q[T]$, resp. $\mathbb{K} = \mathbb{F}_q(T)$. Let \mathbb{M} , resp. \mathbb{I} denote the set of monic polynomials of \mathbb{A} , resp. the set of monic irreducible polynomials of \mathbb{A} .

For any non-zero $H \in \mathbb{A}$, let deg H denote the degree of H, let $\omega(H)$ denote the number of distinct monic irreducible divisors of H and let $|H| = q^{\deg H}$. As usual, if A_1, \ldots, A_r are non-zero polynomials, (A_1, \ldots, A_r) denotes their greatest monic common divisor and for a real number x, [x] denotes the integral part of x.

Let (α, β, γ) be a triple of non-zero elements of the field $\mathbb{K} = \mathbb{F}_q(T)$ and let \mathbb{L} be any field containing \mathbb{K} . If the equation $\alpha x^2 + \beta y^2 + \gamma z^2 = 0$ admits a non-trivial solution $(x, y, z) \in \mathbb{L}^3$, then the quadratic form $\alpha X^2 + \beta Y^2 + \gamma Z^2$ is said to represent zero over the field \mathbb{L} . We say that a quadratic form represents zero if it represents zero over the field \mathbb{K} .

For positive integers m and n, let $H_1(m, n)$ denote the number of pairs (A, B) of square-free, coprime polynomials such that deg A = m, deg B = n

and such that the quadratic form

(f)
$$X^2 - AY^2 - BZ^2$$

represents zero. We first give an asymptotic estimate for the numbers $H_1(m,n)$ when $\max(m,n)\log 2/\log q < \min(m,n)$.

THEOREM A. Let θ be a real number such that $\log 2/\log q < \theta \leq 1$. For strictly positive integers m and n satisfying $\theta \max(m, n) \leq \min(m, n)$, we have

$$H_1(m,n) = \frac{2}{\pi} \left(q-1\right)^3 \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right)$$

if m and n are even, and in all other cases,

$$H_1(m,n) = \frac{1}{\pi} (q-1)^3 \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right),$$

with the O-constants depending only on q and θ . In particular, for even strictly positive integer n,

$$H_1(n,n) = \frac{2}{\pi} (q-1)^3 \frac{q^{2n-1}}{n} + O\left(\frac{q^{2n}}{n^2}\right),$$

and for odd strictly positive integer n,

$$H_1(n,n) = \frac{1}{\pi} (q-1)^3 \frac{q^{2n-1}}{n} + O\left(\frac{q^{2n}}{n^2}\right),$$

with the O-constants depending only on q.

The proof of Theorem A contains all the tools for proving the following theorem which is the polynomial analogous of Guo's theorem.

THEOREM B. Let $N_1(n)$, resp. $M_1(n)$, denote the number of quadratic forms $AX^2 + BY^2 + CZ^2$ that represent zero and whose coefficients A, B, Care square-free and pairwise coprime polynomials of \mathbb{A} such that deg $A \leq n$, deg $B \leq n$, deg $C \leq n$, $ABC \neq 0$, resp. whose coefficients A, B, C are monic, square-free and pairwise coprime polynomials such that deg A = n, deg B = n, deg C = n. Then, for any integer n > 0,

$$\begin{split} M_1(n) &= 2 \bigg\{ \prod_{P \in \mathbb{I}} \bigg(1 + \frac{3}{2|P|} \bigg) \bigg(1 - \frac{1}{|P|} \bigg)^{3/2} \bigg\} \frac{q^{3n}}{\pi^{3/2} n^{3/2}} + O\bigg(\frac{q^{3n}}{n^{5/2}} \bigg), \\ N_1(n) &= \bigg\{ \frac{q^3 (2q^2 + q + 2)}{(q+1)^2} \bigg\} \bigg\{ \prod_{P \in \mathbb{I}} \bigg(1 + \frac{3}{2|P|} \bigg) \bigg(1 - \frac{1}{|P|} \bigg)^{3/2} \bigg\} \frac{q^{3n}}{\pi^{3/2} n^{3/2}} \\ &+ O\bigg(\frac{q^{3n}}{n^{5/2}} \bigg), \end{split}$$

with the O-constants depending only on q.

M. Car

In this case, there are three poles in the sense of [6] and the term

$$\frac{q^{2n}}{n} = \frac{q^n}{n^{1/2}} \cdot \frac{q^n}{n^{1/2}}$$

occurring in Theorem A is replaced by the term

$$\frac{q^{3n}}{n^{3/2}} = \frac{q^n}{n^{1/2}} \cdot \frac{q^n}{n^{1/2}} \cdot \frac{q^n}{n^{1/2}}.$$

Thanks to Weil's theorem on L-functions, the error term in Theorem B is better than that in Guo's theorem. Crucial to the proof is the formula (2.9) below. In order to avoid useless complications, we detail only the proof of Theorem A.

Let D be a square-free monic polynomial. Let $H_D(m, n)$ denote the number of pairs $(A, B) \in \mathbb{A}^2$ with A and B square-free, (A, B) = (A, D) = (B, D) = 1, deg A = m, deg B = n and such that the quadratic form

(f_D)
$$X^2 - ADY^2 - BDZ^2$$

represents zero. Section 3 is devoted to the computation of $H_D(m, n)$. An estimate for this number is given in Theorem 3.9 below. From this estimate, we deduce an estimate for the number H'(m, n) of pairs $(A, B) \in \mathbb{A}^2$ with A and B square-free, deg A = m, deg B = n and such that the quadratic form (f) represents zero. Finally, we get an estimate for the number H(m, n) of pairs $(A, B) \in \mathbb{A}^2$ with deg A = m, deg B = n and such that the quadratic form (f) represents zero. Note that the polynomials A and B counted in H'(m, n) are not supposed to be relatively prime and that there is no restriction for the pairs counted in H(m, n).

Precise results are given in Theorems C and D below.

THEOREM C. Let θ be a real number such that $\log 2/\log q < \theta \leq 1$. Then, for strictly positive integers m and n satisfying $\theta \max(m, n) \leq \min(m, n)$, we have:

(i) if m and n are both even,

$$H'(m,n) = \frac{2}{\pi} (q-1)^3 C(q) \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right),$$

(ii) otherwise,

$$H'(m,n) = \frac{1}{\pi} (q-1)^3 C(q) \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right),$$

with

$$C(q) = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|(|P|+1)} \right),$$

where the O-constants depend only on q and θ .

THEOREM D. Let ρ be a real number such that $3\log 2/2\log q < \rho \leq 1$. Let m and n be strictly positive integers such that $\rho \max(m, n) \leq \min(m, n)$. Then:

(i) if m and n are both even,

$$H(m,n) = \frac{2q(q-1)}{\pi} C(q) \frac{q^{m+n}}{m^{1/2}n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right),$$

(ii) otherwise,

$$H(m,n) = \frac{q(q-1)}{\pi} C(q) \frac{q^{m+n}}{m^{1/2} n^{1/2}} + O\left(\frac{q^{m+n}}{mn}\right),$$

with the O-constants depending only on q and ϱ .

In the second section we study the distribution of the values of some multiplicative functions defined on the set \mathbb{M} of monic polynomials of $\mathbb{F}_q[T]$. Our proofs make use of Weil's theorem on *L*-functions. In the third section, making use of Hooley's idea, we prove an asymptotic estimate for the numbers $H_D(m, n)$, from which we deduce Theorem A. Theorem C is proved in the fourth section, and Theorem D in the fifth section.

Although we do not give explicit values of all constants occurring in this work, these constants are actually computable. Moreover, in general, they depend on q and other parameters. We agree that a constant denoted $\alpha(x_1, \ldots, x_k)$ depends only on q, x_1, \ldots, x_k , or possibly only on x_1, \ldots, x_k , and that a constant denoted by β depends only on q, or possibly is an absolute constant.

In order to simplify notation, in the following, we agree that unless otherwise stated, the polynomials occurring in the sums are *monic and squarefree*.

2. Multiplicative functions on \mathbb{M} . We denote by D_r the open disk formed by the complex numbers z such that |z| < r and we denote by $z^{1/2}$ the determination of the complex function $z \mapsto z^{1/2}$ for which $1^{1/2} = 1$. We note that the function $z \mapsto (1-z)^{-1/2}$ is holomorphic on D_1 .

LEMMA 2.1. Let $z \mapsto h(z)$ be a holomorphic complex-valued function defined over the open disk D_R with R > 1. For $z \in D_1$, let the sequence (a_n) be defined by

(2.1)
$$h(z)(1-z)^{-1/2} = \sum_{n=0}^{\infty} a_n z^n.$$

Let $r \in [0, R[$. Then there exists a constant $\alpha_1(r)$ such that for any integer $n \geq 1$,

(2.2)
$$|a_n - h(1)\pi^{-1/2}n^{-1/2}| \le \alpha_1(r)M(h,r)n^{-3/2},$$

with

(2.3)
$$M(h,r) = \max\{|h(z)|; |z| = r\}.$$

Proof. Apply the Cauchy and Stirling formulae.

Let H be a monic polynomial of positive degree and let χ be a character of the group G_H formed by the invertible elements of the quotient ring $\mathbb{A}/\mathbb{A}H$. The *character modulo* H associated with χ is the multiplicative map ψ_{χ} defined on the ring \mathbb{A} by

$$\psi_{\chi}(R) = \begin{cases} \chi(s(R)) & \text{if } (R,H) = 1, \\ 0 & \text{if } (R,H) \neq 1, \end{cases}$$

s denoting the canonical morphism $\mathbb{A} \to \mathbb{A}/\mathbb{A}H$. In the following, we shall denote by the same symbol χ the character χ of the group G_H and the map ψ_{χ} associated with it. The *arithmetic L-function associated with* χ is the series

(2.4)
$$L(\chi, z) = \sum_{Y \in \mathbb{M}} \chi(Y) z^{\deg Y}$$

Obviously, this series has radius of convergence 1/q. By [3] we know that if χ is different from the unit character, then $L(\chi, z)$ is a polynomial of degree $< \deg H$. We need the results provided by the second part of the following proposition only in the case where χ is quadratic. Since the general case poses no more difficulty, we prove the proposition in the general setting.

PROPOSITION 2.2. (i) Let $\rho \in [0, 1/2[$. Then there exists a constant $\alpha_2(\rho)$ such that for any polynomial K and for any integer n > 0,

(2.5)
$$\left|\sum_{\substack{\deg Y=n\\(Y,K)=1}} 2^{-\omega(Y)} - A\pi^{-1/2}\Theta(K)q^n n^{-1/2}\right| \le \alpha_2(\varrho)\lambda_\varrho(K)q^n n^{-3/2},$$

where

(2.6)
$$A = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|} \right) \left(1 - \frac{1}{|P|} \right)^{1/2},$$

(2.7)
$$\Theta(K) = \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1 + \frac{1}{2|P|} \right)^{-1},$$

(2.8)
$$\lambda_{\varrho}(K) = \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1 - \frac{|P|^{\varrho-1}}{2}\right)^{-1}$$

(ii) There exists a constant α_3 such that for any monic, non-constant polynomial H, any non-unit character χ of the group G_H , any polynomial

K coprime with H and any integer n > 0,

(2.9)
$$\left| \sum_{\substack{(Y,K)=1\\ \deg Y=n}} 2^{-\omega(Y)} \chi(Y) \right| \le \alpha_3 2^{\omega(K)} n^{1/2} q^{n/2} 2^{\deg(H)/2}.$$

Proof. Let H be a monic polynomial, and let χ be a character of G_H . If H = 1, the character modulo H associated with χ is assumed to be the constant map equal to 1. Let

(1)
$$a_n = \sum_{\substack{(M,K)=1 \\ \deg M=n}} 2^{-\omega(M)} \chi(M).$$

The series

(2)
$$f(z) = \sum_{n=0}^{\infty} a_n \left(\frac{z}{q}\right)^n$$

is absolutely convergent in the open disk D_1 . If $z \in D_1$, f(z) may be expanded as an eulerian product:

$$f(z) = \sum_{(M,K)=1} 2^{-\omega(M)} \chi(M) \left(\frac{z}{q}\right)^{\deg M} = \prod_{\substack{P \in \mathbb{I} \\ P \nmid K}} \left(1 + \frac{1}{2} \chi(P) \left(\frac{z}{q}\right)^{\deg P}\right).$$

Hence,

(3)
$$\left(\frac{f(z)}{U(z)}\right)^2 = \prod_{P \in \mathbb{I}} \left(1 + \chi(P)\left(\frac{z}{q}\right)^{\deg P} + \frac{1}{4}\chi(P)^2\left(\frac{z}{q}\right)^{2\deg P}\right),$$

with

(4)
$$U(z) = \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1 + \frac{1}{2} \chi(P) \left(\frac{z}{q} \right)^{\deg P} \right)^{-1}.$$

(i) Assume that H = 1 and $\chi = 1$. Then, for $z \in D_1$,

(5)
$$\prod_{P \in \mathbb{I}} \left(1 - \left(\frac{z}{q}\right)^{\deg P} \right)^{-1} = \sum_{Y \in \mathbb{M}} \left(\frac{z}{q}\right)^{\deg Y} = \frac{1}{1-z},$$

the product on the left-hand side of (5) being absolutely convergent in D_1 . Hence, by (3), for $z \in D_1$,

(6)
$$f(z) = U(z)G(z)^{1/2}(1-z)^{-1/2}$$

where

(7)
$$G(z) = \prod_{P \in \mathbb{I}} \left(1 - \frac{3}{4} \left(\frac{z}{q} \right)^{2 \deg P} - \frac{1}{4} \left(\frac{z}{q} \right)^{3 \deg P} \right).$$

Let $\rho \in [0, 1/2[$. According to Lemma 2.1, since U is holomorphic on D_q and $G^{1/2}$ is holomorphic on $D\sqrt{q}$,

(8)
$$\left| a_n q^{-n} - U(1) \sqrt{\frac{G(1)}{\pi}} n^{-1/2} \right| \le \beta(\varrho) \max\{ |U(z)| |G(z)|^{1/2}; |z| = q^{\varrho} \} n^{-3/2},$$

with $\beta(\varrho)$ a constant.

For $|z| = q^{\varrho}$,

$$\begin{split} |U(z)|^{1/2} &\leq \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1 - \frac{|P|^{\varrho - 1}}{2} \right)^{-1}, \\ |G(z)| &\leq \prod_{P \in \mathbb{I}} (1 + |P|^{2\varrho - 2}), \end{split}$$

and by (5),

$$|G(z)| \le \frac{1 - q^{4\varrho - 3}}{1 - q^{2\varrho - 1}} \le \frac{1}{1 - q^{2\varrho - 1}}.$$

The first part of the proposition is then given by (8).

(ii) Assume that $H \neq 1$ and that χ is different from the unit character. By (2.4),

$$L\left(\chi, \frac{z}{q}\right) = \prod_{P \in \mathbb{I}} \left(1 - \chi(P)\left(\frac{z}{q}\right)^{\deg P}\right)^{-1}$$

and

(9)
$$f(z)^2 = U(z)^2 L\left(\chi, \frac{z}{q}\right) G(z),$$

where

(10)
$$G(z) = \prod_{P \in \mathbb{I}} \left(1 - \frac{3}{4} \chi(P)^2 \left(\frac{z}{q}\right)^{2 \deg P} - \frac{1}{4} \chi(P)^3 \left(\frac{z}{q}\right)^{3 \deg P} \right).$$

Then $G^{1/2}$ is holomorphic on $D\sqrt{q}$.

According to [5, Chapter 2], we associate with χ a non-principal quasicharacter θ of the idele group $\mathbb{J}(\mathbb{K})$ of the field $\mathbb{K} = \mathbb{F}_q(T)$. Let L_{θ} denote the *L*-function associated with the quasi-character θ . Let \mathbb{S} be the union of the infinite place and the places associated with the irreducible divisors of *H*. According to [5, Theorem 3], for any $v \in \mathbb{S}$, there exists a complex number $\varepsilon(v)$, with $|\varepsilon(v)| \in \{0, 1\}$, such that

(11)
$$L(\chi, z) = L_{\theta}(z) \prod_{v \in \mathbb{S}} (1 - \varepsilon(v) z^{\deg v}).$$

According to Weil's theorem, L_{θ} is a polynomial and if L_{θ} is not equal to 1, its roots are algebraic integers of modulus $q^{-1/2}$ (cf. [7, Appendix 5]). By (11),

(12)
$$L\left(\chi, \frac{z}{q}\right) = \prod_{i=1}^{d} (1 - \alpha_i z),$$

with

(13)
$$|\alpha_i| \in \{q^{-1}, q^{-1/2}\},\$$

$$(14) d < \deg H.$$

Let $\delta \in [1/2, 1[$. Let z be a complex number such that $|z| = q^{1-\delta}$. Then, by (9), (4), (10), (12) and (13),

(15)
$$|f(z)| \le m(\delta),$$

with

(16)
$$m(\delta)^2 = (1+q^{1/2-\delta})^d \left\{ \prod_{P \in \mathbb{I}} \left(1+\frac{1}{|P|^{2\delta}} \right) \right\} \left\{ \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1-\frac{1}{2|P|^{\delta}} \right)^{-2} \right\}.$$

Now, by (5),

$$\prod_{P \in \mathbb{I}} \left(1 + \frac{1}{|P|^{2\delta}} \right) = \frac{1 - q^{1 - 4\delta}}{1 - q^{1 - 2\delta}},$$

hence,

$$m(\delta)^2 \le 2^{d+2\omega(K)} (1-q^{1-2\delta})^{-1}.$$

By (2), (15) and the Cauchy formula, we get

(17)
$$|a_n| \le 2^{d/2} 2^{\omega(K)} (1 - q^{1-2\delta})^{-1/2} q^{\delta n}$$

for any $\delta \in [1/2, 1[.$

Now, we suppose that $n \ge 3$ and we choose $\delta = 1/2 + 1/n$. By (17),

(18)
$$|a_n| \le \frac{q}{\sqrt{3(1-q^{-2/3})}} 2^{d/2} 2^{\omega(K)} n^{1/2} q^{n/2}.$$

We remark that (18) remains true for n = 1 or 2, proving the second part of the proposition.

PROPOSITION 2.3. Let $\rho \in [0, 1/2[$. Then there exists a constant $\alpha_4(\rho)$ such that for any polynomial K and any positive integer n,

(2.10)
$$\left|\sum_{\substack{\deg Y=n\\(Y,K)=1}} 2^{-\omega(Y)} \Theta(Y) - \frac{B}{\pi^{1/2}} \Psi(K) \frac{q^n}{n^{1/2}}\right| \le \alpha_4(\varrho) \lambda_{\varrho}(K) \frac{q^n}{n^{3/2}},$$

M. Car

with

(2.11)
$$B = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|+1} \right) \left(1 - \frac{1}{|P|} \right)^{1/2},$$

(2.12)
$$\Psi(K) = \prod_{\substack{P \in \mathbb{I} \\ P \mid K}} \left(1 + \frac{1}{2|P|+1} \right)^{-1}.$$

Proof. As for the above proposition.

PROPOSITION 2.4. Let \mathbb{M}_1 denote the set of square-free monic polynomials. Then

(2.13)
$$\sum_{Y \in \mathbb{M}_1} (\deg Y) |Y|^{-2} = \frac{q^2 + q - 1}{q^2(q - 1)},$$

(2.14)
$$\sum_{Y \in \mathbb{M}_1} 2^{-\omega(Y)} \Theta(Y) \Psi(Y) |Y|^{-2} = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|(|P|+1)} \right).$$

Proof. Let a_n denote the number of square-free monic polynomials of degree n. Then $a_0 = a_1 = 1$ and $a_n = (1 - 1/q)q^n$. Hence,

$$\sum_{Y \in \mathbb{M}_1} (\deg Y) |Y|^{-2} = \frac{1}{q} + \sum_{n=2}^{\infty} n \left(1 - \frac{1}{q} \right) q^{-n} = q^{-2} + (q-1)q^{-2} \sum_{n=1}^{\infty} nq^{-n+1},$$

whence (2.13). Let P be a monic irreducible polynomial. In view of (2.7) and (2.12),

$$\Theta(P)\Psi(P)|P|^{-2} = \left(1 + \frac{1}{2|P|}\right)^{-1} \left(1 + \frac{1}{2|P|+1}\right)^{-1}|P|^{-2} = \frac{1}{|P|(|P|+1)}$$

and (2.14) follows.

PROPOSITION 2.5. Let $\rho \in [0, 1/2[$. Then there exists a constant $\alpha_5(\rho)$ such that for any integer n > 0,

(2.15)
$$\left|\sum_{\deg Y=n} 2^{-\omega(Y)} \lambda_{\varrho}(Y)\right| \le \alpha_5(\varrho) \frac{q^n}{n^{1/2}}.$$

Proof. By a proof which mimics that of Proposition 2.2 one may get an asymptotic estimate for the sum occurring on the left hand side of (2.15) from which one may deduce the announced result.

3. Estimations for $H_D(m,n)$ **and** $Q_D(m,n)$ **.** Let us recall some facts about the polynomial Jacobi symbol. Let $P \in \mathbb{I}$. The Legendre quadratic character modulo P is defined as follows. For $A \in \mathbb{A}$ coprime with P, let

(3.1)
$$\begin{pmatrix} \frac{A}{P} \end{pmatrix} = \begin{cases} 1 & \text{if } A \text{ is a square mod } P, \\ -1 & \text{if } A \text{ is not a square mod } P. \end{cases}$$

The Jacobi symbol is defined as follows. For any monic polynomial D and $A \in \mathbb{A}$ coprime with D, let

(3.2)
$$\left(\frac{A}{D}\right) = \prod_{\substack{P \in \mathbb{I} \\ P \mid D}} \left(\frac{A}{P}\right)^{v_P(D)},$$

 $v_P(D)$ denoting the *P*-adic valuation of *D*.

We extend the map $(\frac{\cdot}{D})$ to all polynomials by setting $(\frac{A}{D}) = 0$ for polynomials A such that $(A, D) \neq 1$. We shall make use of some properties of this symbol collected in the following proposition.

PROPOSITION 3.1. (i) Let $X, Y \in \mathbb{M}$. Then

(3.3)
$$\left(\frac{-1}{X}\right) = \varepsilon^{\deg X},$$

(3.4)
$$\left(\frac{X}{Y}\right)\left(\frac{Y}{X}\right) = \varepsilon^{\deg X \deg Y},$$

with

(3.5)
$$\varepsilon = \varepsilon(q) = (-1)^{(q-1)/2}$$

(ii) Let a be a non-zero element in the field \mathbb{F}_q . Let D be a monic, squarefree polynomial. Then $\left(\frac{a}{D}\right) = -1$ if and only if a is not a square in \mathbb{F}_q and deg D is odd.

Proof. The first part is proved in [2] for irreducible X and Y. The multiplicativity of the symbol gives (3.3) and (3.4) in the general case. Let a be a non-zero element in \mathbb{F}_q . If a is a square in \mathbb{F}_q , then $\left(\frac{a}{P}\right) = 1$ for any $P \in \mathbb{I}$, and $\left(\frac{a}{D}\right) = 1$ for any monic square-free D. Suppose that a is not a square in \mathbb{F}_q . Let α be a root of $T^2 - a$ in an algebraic closure of \mathbb{F}_q . Then

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha).$$

Let $P \in \mathbb{I}$. Then the field $\mathbb{F}_{|P|} = \mathbb{F}_{q^{\deg P}}$ is the splitting field of P. Hence, $\alpha \in \mathbb{F}_{|P|}$ if and only if deg P is even. But $\alpha \in \mathbb{F}_{|P|}$ if and only if a is a square mod P. Hence, $\left(\frac{a}{P}\right) = 1$ if and only if deg P is even. Now, by (3.2), $\left(\frac{a}{D}\right) = -1$ if and only if the number of irreducible divisors of odd degree of D is odd.

Let D be a monic square-free polynomial. We observe that $H_D(m, n) = H_D(n, m)$. Using this symmetry, we may suppose $m \leq n$. Moreover, in the following we shall suppose that

$$(3.6) 1 \le m \le n,$$

and that

(3.7)
$$m + \deg D \le n \, \frac{\log q}{\log 2}$$

Let $\mathbb{X} = \mathbb{X}_D(m, n)$, resp. $\mathbb{Y} = \mathbb{Y}_D(m, n)$, denote the set of $(A, B) \in \mathbb{M}^2$, resp. $(A, B) \in \mathbb{A}^2$, such that

- (1) A and B are square-free,
- (2) (A, D) = 1, (AD, B) = 1,
- (3) $\deg A = m$, $\deg B = n$.

Then $H_D(m, n)$ is the number of $(A, B) \in \mathbb{Y}$ such that the equation

$$(f_D) X^2 - ADY^2 - BDZ^2 = 0$$

admits a non-trivial solution $(x, y, z) \in \mathbb{K}^3$.

Let $\Xi = \Xi_D(m)$, resp. $\Xi' = \Xi'_D(m)$, denote the set of $A \in \mathbb{M}$, resp. $A \in \mathbb{A}$, such that

- (1) A is square-free, coprime with D,
- (2) $\deg A = m$.

If $A \in \Xi$, resp. if $A \in \Xi'$, we denote by \mathbb{X}_A , resp. \mathbb{Y}_A , the set of polynomials B such that $(A, B) \in \mathbb{X}$, resp. $(A, B) \in \mathbb{Y}$.

We recall our convention. Unless otherwise stated, the polynomials occurring in the sums below are monic and square-free.

PROPOSITION 3.2. We have

$$(3.8) \quad 2^{\omega(D)} H_D(m,n) = \sum_{D'D''=D} \left(\frac{-1}{D'}\right) \sum_{(A,B)\in\mathbb{Y}} 2^{-\omega(AB)} \sum_{A'|A} \sum_{B'|B} \left(\frac{AB}{D'}\right) \left(\frac{BD}{A'}\right) \left(\frac{AD}{B'}\right).$$

Proof. Let A and B be square-free non-zero elements of the ring A such that (A, B) = (A, D) = (B, D) = 1. For $P \in \mathbb{I}$, let \mathbb{K}_P denote the P-adic completion of the field K. By the Hasse principle, the quadratic form (f_D) represents zero over K if and only if it represents zero over \mathbb{K}_P , for any $P \in \mathbb{I}$. If $P \in \mathbb{I}$ does not divide ABD, then AD and BD are P-adic units and (f_D) represents zero over \mathbb{K}_P . If $P \in \mathbb{I}$ divides A, then (f_D) represents zero over \mathbb{K}_P if and only if BD is a square modulo P. If $P \in \mathbb{I}$ divides D, then (f_D) represents zero over \mathbb{K}_P if and only if -AB is a square modulo P. Hence, the quadratic form (f_D) represents zero over K if and only if

$$\left\{\prod_{\substack{P\in\mathbb{I}\\P\mid A}}\left\{1+\left(\frac{BD}{P}\right)\right\}\right\}\left\{\prod_{\substack{P\in\mathbb{I}\\P\mid B}}\left\{1+\left(\frac{AD}{P}\right)\right\}\right\}\left\{\prod_{\substack{P\in\mathbb{I}\\P\mid D}}\left\{1+\left(\frac{-AB}{P}\right)\right\}\right\}\right\}$$
$$=2^{\omega(ABD)}$$

It follows that

$$2^{\omega(D)}H_D(m,n) = \sum_{(A,B)\in\mathbb{Y}} 2^{-\omega(AB)} \sum_{D'|D} \left(\frac{-AB}{D'}\right) \sum_{A'|A} \left(\frac{BD}{A'}\right) \sum_{B'|B} \left(\frac{AD}{B'}\right).$$

We get (3.8) by interchanging the order of summation.

Following Hooley's idea, we split the sum $H_D(m, n)$ into subsums corresponding to different types of divisors. We need a new notation. For non-zero polynomials U, V and W we set

(3.9) $\delta(U, V, W) = \varepsilon^{\deg U + \deg U \deg V + \deg V \deg W + \deg W \deg U}.$

PROPOSITION 3.3. We have

(3.10)
$$H_D(m,n) = S_1(m,n) + S_2(m,n) + S_3(m,n),$$

where

(3.11)
$$2^{\omega(D)}S_1(m,n) = \kappa(m,n,\deg D)(q-1)^2 \sum_{(A,B)\in\mathbb{X}} 2^{-\omega(AB)}$$

with

(3.14) T(A B)

(3.12)
$$\kappa(m, n, \deg D) = \begin{cases} 2 & \text{if } m + \deg D \text{ and } n + \deg D \text{ are even,} \\ 1 & \text{otherwise,} \end{cases}$$

(3.13)
$$2^{\omega(D)}S_2(m,n) = (q-1)^2 \sum_{(A,B)\in\mathbb{X}} 2^{-\omega(AB)}T(A,B),$$

$$(3.14) \quad \tau(X,D)$$

$$= \begin{cases} 2 \sum_{\substack{B'|B \\ B' \neq 1 \\ \deg B' \equiv 0 \mod 2}} \left(\frac{AD}{B'}\right) & if m + \deg D \ and n + \deg D \ are \ even, \\ \sum_{\substack{B'|B \\ B' \neq 1}} \left(\frac{AD}{B'}\right) & if m + \deg D \ is \ odd, \\ \sum_{\substack{B'|B \\ B' \neq 1}} \left(\frac{AD}{B'}\right) & if m + \deg D \ is \ even \ and \ n + \deg D \ is \ odd, \end{cases}$$

$$(3.15) \quad 2^{\omega(D)}S_3(m,n)$$

$$= \sum_{\substack{D'D''=D \\ 1\neq D' \neq D}} \sum_{\substack{A'A'' \in \Xi' \\ D'A' \neq 1 \\ \deg(D''A'') \neq 0}} 2^{-\omega(A'A'')} \left(\frac{A''}{D'}\right) \left(\frac{D''}{A'}\right) \tau(D',A',A''),$$

$$(3.16) \quad \tau(D',A',A'')$$

$$= \sum_{B \in \mathbb{Y}_{A'A''}} 2^{-\omega(B)} \sum_{\substack{B'' \in \mathbb{A}\\B'B''=B}} \delta(D',A',B') \left(\frac{B''}{D'A'}\right) \left(\frac{A''D''}{B'}\right).$$

Proof. If X is a non-zero element of the ring A, we denote by X^* the monic polynomial such that X and X^* generate the same ideal. We split the right hand side of (3.8) into three subsums $2^{\omega(D)}S_i(m,n) = 2^{\omega(D)}S_i$, $1 \leq i \leq 3$, corresponding to different 3-tuples (D', A', B') of divisors. The sum $2^{\omega(D)}S_1$ which will be the main term contains only for each $(A, B) \in \mathbb{Y}$ the triple (1, 1, 1) and the triple (D, A^*, B^*) , that is to say,

$$2^{\omega(D)}S_1 = \sum_{(A,B)\in\mathbb{Y}} 2^{-\omega(AB)} \left\{ 1 + \left(\frac{-1}{D}\right) \left(\frac{AB}{D}\right) \left(\frac{BD}{A^*}\right) \left(\frac{AD}{B^*}\right) \right\}.$$

Writing A and B as the product of a monic polynomial by a non-zero constant, we get

$$2^{\omega(D)}S_1 = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \times \sum_{a\in\mathbb{F}_q^*} \sum_{b\in\mathbb{F}_q^*} \left\{ 1 + \left(\frac{-1}{D}\right) \left(\frac{ab}{D}\right) \left(\frac{b}{U}\right) \left(\frac{a}{V}\right) \left(\frac{UV}{D}\right) \left(\frac{VD}{U}\right) \left(\frac{UD}{V}\right) \right\}.$$

Making use of (3.3) and (3.4), we get

$$2^{\omega(D)}S_1 = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{a\in\mathbb{F}_q^*} \sum_{b\in\mathbb{F}_q^*} \{1+\varepsilon^{(m+n+1)\deg D+mn}\} \left(\frac{a}{DV}\right) \left(\frac{b}{DU}\right).$$

Suppose that $m + \deg D$ and $n + \deg D$ are both even. Then

$$\{1 + \varepsilon^{(m+n+1)\deg D + mn}\} = 2$$

and making use of Proposition 3.1(ii) we get

$$2^{\omega(D)-1}S_1 = (q-1)^2 \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)}.$$

Suppose that $m + \deg D$ is odd. Then, by Proposition 3.1(ii), for any $U \in \Xi$ and any $b \in \mathbb{F}_q^*$,

$$\left(\frac{b}{DU}\right) = \begin{cases} 1 & \text{if } b \text{ is a square,} \\ -1 & \text{if } b \text{ is not a square} \end{cases}$$

Hence, for any $U \in \Xi$,

$$\sum_{b \in \mathbb{F}_q^*} \left(\frac{b}{DU} \right) = 0$$

and

$$2^{\omega(D)}S_1 = (q-1)^2 \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)}.$$

The case where $n + \deg D$ is odd is similar.

The sum $2^{\omega(D)}S_2$ contains for each $(A, B) \in \mathbb{Y}$ the triples (1, 1, B') with $B' \neq 1$ and the triples (D, A^*, B') with $B' \neq B^*$. Then, writing A, resp. B, as the product of a monic polynomial by a non-zero constant, we get

$$2^{\omega(D)}S_{2} = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \bigg\{ \sum_{\substack{V'V''=V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \sum_{\substack{a\in\mathbb{F}_{q}^{*} \ b\in\mathbb{F}_{q}^{*}}} \sum_{b\in\mathbb{F}_{q}^{*}} \left(\frac{a}{V'}\right) + \left(\frac{-1}{D}\right) \sum_{\substack{V'V''=V\\V''\neq 1}} \left(\frac{UV}{D}\right) \left(\frac{VD}{U}\right) \left(\frac{UD}{V'}\right) \\ \times \sum_{a\in\mathbb{F}_{q}^{*} \ b\in\mathbb{F}_{q}^{*}} \sum_{b\in\mathbb{F}_{q}^{*}} \left(\frac{ab}{D}\right) \left(\frac{a}{V'}\right) \left(\frac{b}{U}\right) \bigg\}.$$

Since

$$\left(\frac{UD}{V'}\right) = \left(\frac{UD}{V'}\right) \left(\frac{UD}{V''}\right)^2 = \left(\frac{UD}{V}\right) \left(\frac{UD}{V''}\right),$$

and similarly,

$$\left(\frac{a}{V'}\right) = \left(\frac{a}{V}\right) \left(\frac{a}{V''}\right),$$

we obtain

$$2^{\omega(D)}S_{2} = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \bigg\{ \sum_{\substack{V'V''=V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \sum_{\substack{a\in\mathbb{F}_{q}^{*} \ b\in\mathbb{F}_{q}^{*}}} \sum_{b\in\mathbb{F}_{q}^{*}} \left(\frac{a}{V'}\right) \\ + \left(\frac{-1}{D}\right) \sum_{\substack{V'V''=V\\V''\neq 1}} \left(\frac{UV}{D}\right) \left(\frac{VD}{U}\right) \left(\frac{UD}{V}\right) \left(\frac{UD}{V''}\right) \\ \times \sum_{a\in\mathbb{F}_{q}^{*} \ b\in\mathbb{F}_{q}^{*}} \sum_{b\in\mathbb{F}_{q}^{*}} \left(\frac{ab}{D}\right) \left(\frac{a}{V'}\right) \left(\frac{a}{V''}\right) \left(\frac{b}{U}\right) \bigg\}.$$

Making use of (3.3) and (3.4), we get

$$2^{\omega(D)}S_2 = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'V''=V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \\ \times \sum_{a\in\mathbb{F}_q^*} \sum_{b\in\mathbb{F}_q^*} \left(\frac{a}{V'}\right) \left\{1 + \varepsilon^{(m+n+1)\deg D + mn}\left(\frac{a}{DV}\right)\left(\frac{b}{DU}\right)\right\}.$$

Assume that $m + \deg D$ and $n + \deg D$ are both even. Then, as above,

$$2^{\omega(D)-1}S_2 = \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'V''=V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \sum_{\substack{a\in\mathbb{F}_q^*\\b\in\mathbb{F}_q^*}} \sum_{b\in\mathbb{F}_q^*} \left(\frac{a}{V'}\right)$$

M. Car

and

$$2^{\omega(D)-1}S_2 = (q-1)^2 \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'|V\\V'\neq 1\\ \deg V'\equiv 0 \bmod 2}} \left(\frac{UD}{V'}\right).$$

Assume that $m + \deg D$ is odd. Then, as above,

$$2^{\omega(D)}S_2 = (q-1)\sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'|V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \sum_{\substack{a\in\mathbb{F}_q^*\\V'\neq 1}} \left(\frac{a}{V'}\right)$$

and

$$2^{\omega(D)}S_2 = (q-1)^2 \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'|V\\V'\neq 1\\ \deg V'\equiv 0 \bmod 2}} \left(\frac{UD}{V'}\right).$$

Assume that $n + \deg D$ is odd and that $m + \deg D$ is even. Then, as above,

$$2^{\omega(D)}S_{2} = (q-1)\sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'|V\\V'\neq 1}} \left(\frac{UD}{V'}\right) \sum_{a\in\mathbb{F}_{q}^{*}} \left\{ \left(\frac{a}{V'}\right) + \left(\frac{a}{DVV'}\right) \right\},$$
$$2^{\omega(D)}S_{2} = (q-1)^{2} \sum_{(U,V)\in\mathbb{X}} 2^{-\omega(UV)} \sum_{\substack{V'|V\\V'\neq 1}} \left(\frac{UD}{V'}\right).$$

This completes the proof of (3.13).

The sum $2^{\omega(D)}S_3$ contains the remaining terms, that is to say, all the 3-tuples (D', A', B') of monic divisors such that $D'A' \neq 1$, $D'A' \neq DA^*$. Then, writing D = D'D'', A = A'A'', B = B'B'', and making use once more of (3.3) and (3.4), we get

$$2^{\omega(D)}S_{3} = \sum_{\substack{D'D''=D\\1\neq D'\neq D}} \sum_{\substack{(A,B)\in\mathbb{Y}\\D'A'\neq D}} 2^{-\omega(AB)} \sum_{\substack{A'A''=A\\D'A'\neq A}} \binom{A''}{D'} \binom{D''}{A'}$$
$$\times \sum_{\substack{B'B''=B\\B''\in\mathbb{A}}} \delta(D',A',B') \binom{B''}{A'D'} \binom{A''D''}{B'},$$

proving (3.15).

PROPOSITION 3.4. There exists a constant β_1 such that (3.17) $|S_2(m,n)| \leq \beta_1 m^{1/2} q^{n+m/2} 2^{n/2}.$

1

$$\begin{array}{l} Proof. \text{ In view of (3.13) and (3.14), we have} \\ 2^{\omega(D)-1}|S_2(m,n)| \\ \leq (q-1)^2 \sum_{\substack{\deg W \leq n \\ W \neq 1 \\ (W,D)=1}} 2^{-\omega(W)} \sum_{\substack{\deg Y = n - \deg W \\ (WD,Y)=1}} 2^{-\omega(Y)} \left| \sum_{\substack{\deg A = m \\ (A,WYD)=1}} 2^{-\omega(A)} \left(\frac{A}{W} \right) \right|. \end{array}$$

By (2.9), if $W \neq 1$,

$$\left|\sum_{\substack{\deg A=m\\(A,WYD)=1}} 2^{-\omega(A)} \left(\frac{A}{W}\right)\right| \le \alpha_3 2^{\omega(YD)} m^{1/2} q^{m/2} 2^{\deg(W)/2}$$

hence

ъ

$$|S_2(m,n)| \le 2(q-1)^2 \alpha_3 \frac{2^{1/2}}{2^{1/2}-1} m^{1/2} q^{n+m/2} 2^{n/2},$$

whence (3.17) follows with

$$\beta_1 = \alpha_3 \frac{2^{3/2}}{2^{1/2} - 1} (q - 1)^2.$$

PROPOSITION 3.5. There exists a constant β_2 such that for monic $D' \mid D$, $A \in \Xi, a \in \mathbb{F}_q^*$ and monic A' | A such that $\deg(D'A') \neq 0, \deg(D'A') \neq 0$ $\deg(DA)$, we have

(3.18)
$$|\tau(D', A', aA/A')| \le \beta_2 n^{1/2} q^{3n/4} 2^{\omega(AD) + \deg(AD)/4}$$

moreover, if $\deg(D'A')$ is odd, then $\tau(D', A', aA/A') = 0$.

Proof. We set D = D'D'', A = A'A''. We note that D' and D'' are square-free and coprime polynomials of positive degree. By (3.16),

$$\tau(D',A',aA'') = \sum_{B\in\mathbb{X}_A} 2^{-\omega(B)} \sum_{B'B''=B} \delta(D',A',B') \left(\frac{B''}{D'A'}\right) \left(\frac{aA''D''}{B'}\right) \sum_{b\in\mathbb{F}_q^*} \left(\frac{b}{D'A'}\right).$$

In view of Proposition 3.1(ii), if $\deg(D'A')$ is odd, then the last sum is 0 and $\tau(D', A', aA'') = 0$. We suppose deg(D'A') even. Then

$$\tau(D', A', aA'') = (q-1) \sum_{B \in \mathbb{X}_A} 2^{-\omega(B)} \sum_{B'B''=B} \delta(D', A', B') \left(\frac{B''}{D'A'}\right) \left(\frac{aA''D''}{B'}\right).$$

Let h be a non-negative integer such that

(1)h < n. We divide $\tau(D', A', aA'')$ into two parts according as deg $B' \leq h$ or deg B' > h. Making use of (3.4), we get

(2)
$$\tau(D', A', aA'') = (q-1)(\tau_1(D', A', A'') + \tau_2(D', A', a, A'')),$$

with

(3)
$$\tau_1(D', A', A'')$$

$$= \sum_{\substack{\deg B' \le h \\ (B', AD) = 1}} \delta(D', A', B') 2^{-\omega(B')} \left(\frac{aA''D''}{B'}\right) \sum_{\substack{\deg B'' = n - \deg B' \\ (B'', DAB') = 1}} 2^{-\omega(B'')} \left(\frac{B''}{D'A'}\right),$$

(4) $\varepsilon^{\deg D'(1+\deg A')+n(m+\deg D)}\tau_2(D',A',a,A'')$

$$= \sum_{\substack{\deg B'' < n-h \\ (B''AD)=1}} 2^{-\omega(B'')} \varepsilon^{(m+\deg D) \deg(B'')} \left(\frac{B''}{D'A'}\right)$$
$$\times \sum_{\substack{\deg B'=n-\deg B'' \\ (B',DAB'')=1}} 2^{-\omega(B')} \left(\frac{a}{B'}\right) \left(\frac{B'}{D''A''}\right).$$

(I) Let $W \in \mathbb{M}$ be such that deg $W \leq h$. In view of (2.9),

$$\left|\sum_{\substack{\deg Y = n - \deg W \\ (Y, DAW) = 1}} 2^{-\omega(Y)} \left(\frac{Y}{D'A'}\right)\right| \le \alpha_3 n^{1/2} q^{n/2} 2^{\omega(D'A''W) + \deg(D'A')/2} |W|^{-1/2};$$

hence, by (3) and (3.9),

(5)
$$|\tau_1(D', A', A'')| \le \alpha_3 \frac{q^{1/2}}{q^{1/2} - 1} n^{1/2} q^{n/2 + h/2} 2^{\omega(AD) + \deg(D'A')/2}.$$

(II) Let $W \in \mathbb{M}$ be such that deg W < n - h. According to (2.9),

$$\left|\sum_{\substack{\deg Y = n - \deg W \\ (Y, DAW) = 1}} 2^{-\omega(Y)} \left(\frac{Y}{A''D''}\right)\right| \le \alpha_3 n^{1/2} q^{n/2} 2^{\omega(A'D'W) + \deg(A''D'')/2} |W|^{-1/2}.$$

Since the sign of $\left(\frac{a}{B'}\right)$ depends at most on the degree of B', by (4) we have

(6)
$$|\tau_2(D', A', a, A'')| \le \alpha_3 \frac{1}{q^{1/2} - 1} n^{1/2} q^{n - h/2} 2^{\omega(AD) + \deg(A''D'')/2}$$

Let η be defined by

(7)
$$q^{\eta} = q^{n/2} 2^{(\deg A''D'' - \deg A'D')/2}.$$

In view of (3.6) and (3.7), we have $\eta < n$ and we may choose $h = [\eta]$. With this choice, by (2), (5) and (6),

$$|\tau(D', A', aA'')| \le \beta_2 n^{1/2} q^{3n/4} 2^{\omega(AD) + \deg(AD)/4}$$

with

$$\beta_2 = 2\alpha_3(q-1) \frac{q^{1/2}}{q^{1/2}-1}.$$

This gives (3.18).

PROPOSITION 3.6. We have

(3.19)
$$|S_3(m,n)| \le \beta_2(q-1)(m+1)2^{\omega(D)+\deg(D)/4}n^{1/2}q^{m+3n/4}2^{m/4}.$$

Proof. By (3.15) and the definition of the sets Ξ and Ξ' ,

 $2^{\omega(D)}S_3(m,n)$

$$= \sum_{\substack{D'D''=D\\1\neq D'\neq D}} \sum_{\substack{A'A''\in\Xi\\D'A'\neq 1\\D''A''\neq 1}} 2^{-\omega(A'A'')} \sum_{a\in\mathbb{F}_q^*} \left(\frac{aA''}{D'}\right) \left(\frac{D''}{A'}\right) \tau(D',A',aA'').$$

We conclude by applying (3.18).

Let

(3.20)
$$S(m,n) = \sum_{(X,Y) \in \mathbb{X}(m,n)} 2^{-\omega(XY)}.$$

PROPOSITION 3.7. Let $\rho \in [0, 1/2[$. Then there exists a constant $\beta_3(\rho)$ such that

(3.21)
$$\left| S(m,n) - \left(1 - \frac{1}{q}\right) \frac{q^{m+n}}{\pi m^{1/2} n^{1/2}} \Theta(D) \Psi(D) \right| \le \beta_3(\varrho) \lambda_\varrho(D) \frac{q^{m+n}}{m^{1/2} n^{1/2}} \left(\frac{1}{m} + \frac{1}{n}\right)$$

with $\Theta(D)$, $\Psi(D)$ and $\lambda_{\varrho}(D)$ defined respectively by (2.7), (2.12) and (2.8).

Proof. In view of (3.20) and the definition of the set $\mathbb{X}(m, n)$,

$$S(m,n) = \sum_{\substack{\deg X = m \\ (X,D)=1}} 2^{-\omega(X)} \sum_{\substack{\deg Y = n \\ (XD,Y)=1}} 2^{-\omega(Y)}$$

Let $\rho \in [0, 1/2[$. In view of (2.5), (2.10) and (2.15),

$$\left| S(m,n) - \frac{AB}{\pi} \Theta(D) \Psi(D) \frac{q^{m+n}}{m^{1/2} n^{1/2}} \right|$$

$$\leq \frac{q^{m+n}}{m^{1/2} n^{1/2}} \lambda_{\varrho}(D) \left(\frac{\alpha_4(\varrho)}{\pi^{1/2}} A \Theta(D) \frac{1}{m} + \frac{\alpha_2(\varrho) \alpha_5(\varrho)}{n} \right),$$

with A and B defined by (2.6) and (2.11), and Θ and Ψ defined by (2.7) and (2.12). An easy computation leads to

$$AB = 1 - \frac{1}{q}.$$

In view of (2.7), we have $0 < \Theta(D) \le 1$, whence (3.21) follows with

$$\beta_3(\varrho) = \max(\alpha_4(\varrho)A\pi^{-1/2}, \alpha_2(\varrho)\alpha_5(\varrho)).$$

We summarize what has been proved in this section in the following theorem.

THEOREM 3.9. Let D be a square-free monic polynomial and let m and n be integers such that $1 \le m \le n$ and

$$m + \deg D \le n \, \frac{\log q}{\log 2}.$$

Then, if $m + \deg D$ and $n + \deg D$ are even,

$$\left| H_D(m,n) - (q-1)^3 2^{1-\omega(D)} \frac{q^{m+n-1}}{\pi m^{1/2} n^{1/2}} \Theta(D) \Psi(D) \right|$$

 $\leq \beta_1 m^{1/2} q^{n+m/2} 2^{n/2} + 2(q-1)\beta_2 2^{\omega(D) + \deg(D)/4} m n^{1/2} q^{m+3n/4} 2^{m/4}$
 $+ (q-1)^2 2^{1-\omega(D)} \beta_3 \left(\frac{1}{4}\right) \lambda_{1/4}(D) \frac{q^{m+n}}{m^{1/2} n^{1/2}} \left(\frac{1}{m} + \frac{1}{n}\right),$

otherwise,

$$\begin{aligned} \left| H_D(m,n) - (q-1)^3 2^{-\omega(D)} \frac{q^{m+n-1}}{\pi m^{1/2} n^{1/2}} \Theta(D) \Psi(D) \right| \\ &\leq \beta_1 m^{1/2} q^{n+m/2} 2^{n/2} + 2(q-1) \beta_2 2^{\omega(D) + \deg(D)/4} m n^{1/2} q^{m+3n/4} 2^{m/4} \\ &+ (q-1)^2 2^{-\omega(D)} \beta_3 \left(\frac{1}{4}\right) \lambda_{1/4}(D) \frac{q^{m+n}}{m^{1/2} n^{1/2}} \left(\frac{1}{m} + \frac{1}{n}\right). \end{aligned}$$

For D = 1, this theorem gives a more precise version of Theorem A.

4. Estimations for H'(m, n). First, we recall that H'(m, n) is the number of pairs (A, B) of square-free elements of the ring $\mathbb{A} = \mathbb{F}_q[T]$ such that deg A = m, deg B = n and such that the quadratic form

(f)
$$X^2 - AY^2 - BZ^2$$

represents zero.

THEOREM 4.1. Let θ be a real number with $\log 2/\log q < \theta \leq 1$. Let m and n be strictly positive integers such that $\theta \max(m, n) \leq \min(m, n)$. Then, if m and n are both even,

$$H'(m,n) - \frac{2}{\pi} (q-1)^3 C \left. \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} \right| \le \beta_6(\theta) \left. \frac{q^{m+n}}{n^2} \right|,$$

otherwise,

$$\left| H'(m,n) - \frac{1}{\pi} (q-1)^3 C \frac{q^{m+n-1}}{m^{1/2} n^{1/2}} \right| \le \beta_6(\theta) \frac{q^{m+n}}{n^2},$$

with

$$C = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|(|P|+1)} \right)$$

and $\beta_6(\theta)$ a constant.

Proof. Let m and n be strictly positive integers such that $\theta n \leq m \leq n$. Let (A, B) be a pair of square-free elements of the ring \mathbb{A} and let $D = \gcd(A, B)$. Then (A, B) is counted in H'(m, n) if and only if (A/D, B/D) is counted in $H_D(m - \deg D, n - \deg D)$. Hence,

(1)
$$H'(m,n) = \sum_{\deg D \le m} H_D(m - \deg D, n - \deg D).$$

Let

(2)
$$\mu = \min\left(\left[\frac{m}{2}\right], \left[n - m\frac{\log 2}{\log q}\right]\right)$$

Obviously, for any monic D,

$$H_D(m - \deg D, n - \deg D) \le (q-1)^2 q^{m+n-2\deg D},$$

and by (1),

(3)
$$0 \le H'(m,n) - \overline{H}(m,n) \le (q-1)q^{m+n-\mu},$$

where

(4)
$$\overline{H}(m,n) = \sum_{\deg D \le \mu} H_D(m - \deg D, n - \deg D).$$

If deg $D \le \mu$, then $m \le (n - \deg D) \frac{\log q}{\log 2}$ and we may apply Theorem 3.9 to $H_D(m - \deg D, n - \deg D)$. Taking (2) into account we get

(5)
$$\left|\overline{H}(m,n) - \frac{\chi}{\pi} (q-1)^3 q^{m+n-1} H^*(m,n)\right| \le \Delta(m,n),$$

where

(6)
$$\chi = \chi(m, n) = \begin{cases} 2 & \text{if } m \text{ and } n \text{ are both even,} \\ 1 & \text{if not,} \end{cases}$$

(7)
$$H^*(m,n) = \sum_{\deg D \le \mu} \frac{2^{-\omega(D)} |D|^{-2} \Theta(D) \Psi(D)}{(m - \deg D)^{1/2} (n - \deg D)^{1/2}}$$

(8)
$$\Delta(m,n) = \beta_1 m^{1/2} q^{n+m/2} 2^{n/2} \sum_{\deg D \le \mu} |D|^{-3/2} 2^{-\deg(D)/2} + \beta_4 n^{3/2} q^{m+3n/4} 2^{m/4} \sum_{\deg D \le \mu} 2^{\omega(D)} |D|^{-7/4} + \beta_5 \frac{q^{m+n}}{m^{1/2} n^{1/2}} \left(\frac{1}{m} + \frac{1}{n}\right) \sum_{\deg D \le \mu} \lambda_{1/4}(D) 2^{-\omega(D)} |D|^{-2}$$

with

$$\beta_4 = 2(q-1)\beta_2, \quad \beta_5 = 8(q-1)^2\beta_3(1/4).$$

We have

$$\sum_{\deg D \le \mu} 2^{\omega(D)} |D|^{-7/4} \le \prod_{P \in \mathbb{I}} \left(1 + \frac{2}{|P|^{7/4}} \right) = p_1,$$
$$\sum_{\deg D \le \mu} \lambda_{1/4}(D) 2^{-\omega(D)} |D|^{-2} \le \prod_{P \in \mathbb{I}} \left(1 + \frac{\lambda_{1/4}(P)}{2|P|^2} \right) = p_2,$$

these products being convergent since $1 \le \lambda_{1/4}(P) \le 2/(2-q^{-3/4})$. Hence,

(9)
$$\Delta(m,n) \leq \beta_1 \frac{(2q)^{1/2}}{(2q)^{1/2} - 1} m^{1/2} q^{n+m/2} 2^{n/2} + \beta_4 p_1 n^{3/2} q^{m+3n/4} 2^{m/4} + \beta_5 p_2 \frac{q^{m+n}}{m^{1/2} n^{1/2}} \left(\frac{1}{m} + \frac{1}{n}\right).$$

Now,

$$\begin{split} & \left| H^*(m,n) - \frac{1}{m^{1/2} n^{1/2}} \sum_{\deg D \le \mu} 2^{-\omega(D)} |D|^{-2} \Theta(D) \Psi(D) \right| \\ & \le \frac{2}{1 + 2^{1/2}} \left(\frac{1}{m^{3/2} n^{1/2}} + \frac{2^{1/2}}{m^{1/2} n^{3/2}} \right) \sum_{\deg D \le \mu} \deg D \, 2^{-\omega(D)} |D|^{-2} \Theta(D) \Psi(D). \end{split}$$

In view of (2.7) and (2.12), we bound $\Theta(D)$ and $\Psi(D)$ by 1. Hence, by (2.13) and (2.14),

$$\left| H^*(m,n) - \frac{C}{m^{1/2}n^{1/2}} \right| \le \frac{1}{q-1} q^{-\mu} m^{-1/2} n^{-1/2} + \frac{2^{3/2}(q^2+q-1)}{(1+2^{1/2})q^2(q-1)} m^{-3/2} n^{-1/2},$$

with

$$C = \prod_{P \in \mathbb{I}} \left(1 + \frac{1}{2|P|(|P|+1)} \right).$$

We get the expected result with (3), (6) and (9).

5. Estimations for H(m, n). We recall that H(m, n) is the number of pairs (A, B) of elements of the ring $\mathbb{A} = \mathbb{F}_q[T]$ such that deg A = m, deg B = n and such that the quadratic form

(f)
$$X^2 - AY^2 - BZ^2$$

represents zero.

THEOREM 5.1. Let ρ be a real number such that $3 \log 2/2 \log q < \rho \leq 1$. Let m and n be strictly positive integers such that $\rho \max(m, n) \leq \min(m, n)$. Then, if m and n are both even,

$$\left| H(m,n) - \frac{2Cq(q-1)q^{m+n}}{\pi m^{1/2}n^{1/2}} \right| \le \beta_7(\varrho) \, \frac{q^{m+n}}{n^2},$$

otherwise,

$$\left| H(m,n) - \frac{Cq(q-1)q^{m+n}}{\pi m^{1/2}n^{1/2}} \right| \le \beta_7(\varrho) \, \frac{q^{m+n}}{n^2},$$

with $\beta_7(\varrho)$ a constant. In particular, for any even integer n > 0,

$$\left| H(n,n) - \frac{2Cq(q-1)q^{2n}}{\pi n} \right| \le \beta_7(1) \frac{q^{2n}}{n^2},$$

and for any odd integer n > 0,

$$\left| H(n,n) - \frac{Cq(q-1)q^{2n}}{\pi n} \right| \le \beta_7(1) \frac{q^{2n}}{n^2}.$$

Proof. Let m and n be integers such that $\rho n \leq m \leq n$. Let (A, B) be a pair of non-zero elements of \mathbb{A} . Then A and B are uniquely written as $A = A'U^2$, $B = B'V^2$ with A' and B' square-free, U and V monic. Moreover, (A, B) is counted in H(m, n) if and only if (A', B') is counted in $H'(m - 2 \deg U, n - 2 \deg V)$. Hence,

(1)
$$H(m,n) = \sum_{2 \deg U \le m} \sum_{2 \deg V \le n} H'(m-2 \deg U, n-2 \deg V).$$

Obviously, for any pair occurring in H(m, n),

$$H'(m-2\deg U, n-2\deg V) \le (q-1)^2 q^{m+n-2\deg U-2\deg V}$$

Let \mathcal{E}' denote the set of pairs (U, V) of monic polynomials U and V such that $2 \deg U \leq m/3$ and $2 \deg V \leq n/3$. We note that for $(U, V) \in \mathcal{E}'$, $\min(m-2 \deg U, n-2 \deg V) > 0$. Moreover,

(2)
$$\sum_{\substack{2 \deg U \le m \\ 2 \deg V \le n \\ (U,V) \notin \mathcal{E}'}} H'(m - 2 \deg U, n - 2 \deg V) \le q^{m+n+2} (q^{-m/6} + q^{-n/6}).$$

Let $\theta = \frac{2}{3}\rho$. We note that $\log 2/\log q < \theta \leq 1$. Let \mathcal{E} denote the set of pairs $(U, V) \in \mathcal{E}'$ such that

(3)
$$\min(m - 2\deg U, n - 2\deg V) \ge \theta \max(m - 2\deg U, n - 2\deg V).$$

If a pair $(U, V) \in \mathbb{M} \times \mathbb{M}$ does not satisfy (3), then either $2 \deg V \ge n - m + 2 \deg U$ and in this case $2 \deg V > n - \theta m + 2\theta \deg U \ge n - \theta m$, or $2 \deg V < n - m + 2 \deg U$ and in this case $2 \deg U > m - \theta n + 2\theta \deg V \ge m - \theta n$.

Hence,

(4)
$$\sum_{\substack{(U,V)\in\mathcal{E}'\\(U,V)\notin\mathcal{E}}} H'(m-2\deg U, n-2\deg V) \le q^{m+n+2}(q^{-(n-\theta m)/2} + q^{-(m-\theta n)/2}).$$

Let

(5)
$$\overline{H}(m,n) = \sum_{(U,V)\in\mathcal{E}} H'(m-2\deg U, n-2\deg V).$$

Then, by (2) and (4),

(6)
$$|H(m,n) - \overline{H}(m,n)| \le 4q^{m+n+2-\varrho n/6}$$

If $(U, V) \in \mathcal{E}$, then

 $\min(m-2\deg U, n-2\deg V) \ge \theta \max(m-2\deg U, n-2\deg V) > 0$ and we may apply Theorem 4.1 to $H'(m-2\deg U, n-2\deg V)$, obtaining

(7)
$$\left| \overline{H}(m,n) - \frac{\chi(m,n)C(q-1)^3}{\pi} q^{m+n-1} H^*(m,n) \right| \le \beta'(\varrho) \frac{q^{m+n}}{n^2},$$

with

(8)
$$H^*(m,n) = \sum_{(U,V)\in\mathcal{E}} |U|^{-2} |V|^{-2} (m-2\deg U)^{-1/2} (n-2\deg V)^{-1/2},$$

 $\chi(m,n)$ defined as in the proof of Theorem 4.1 and $\beta'(\varrho)$ a constant. By easy computations we get

(9)
$$0 \le H^*(m,n) - \sum_{(U,V)\in\mathcal{E}} |U|^{-2} |V|^{-2} m^{-1/2} n^{-1/2} \le \beta''(\varrho) n^{-2},$$

with $\beta''(\varrho)$ a constant. Finally, as above we get

$$\left|\sum_{(U,V)\in\mathbb{M}\times\mathbb{M}}|U|^{-2}|V|^{-2} - \sum_{(U,V)\in\mathcal{E}}|U|^{-2}|V|^{-2}\right| \le 2\left(\frac{q}{q-1}\right)^2 q^{-(m-\theta n)/2} \le 2\left(\frac{q}{q-1}\right)^2 q^{-\varrho n/6}.$$

We conclude by applying (6), (7) and (9).

References

- C. R. Guo, On solvability of ternary quadratic forms, Proc. London Math. Soc. (3) 70 (1995), 241–263.
- H. Hasse, Number Theory, 3rd ed., Grundlehren Math. Wiss. 229, Springer, 1980, Part I, Chap. 5, 100–103.

- [3] D. R. Hayes, The distribution of irreducibles in GF[q, x], Trans. Amer. Math. Soc. 117 (1965), 101–127.
- C. Hooley, On ternary quadratic forms that represent zero, Glasgow Math. J. 35 (1993), 13–23.
- G. Rhin, Répartition modulo 1 dans un corps de séries formelles sur un corps fini, Dissertationes Math. 95 (1972).
- [6] J.-P. Serre, Spécialisation des éléments de $Br_2(Q(T_1, \ldots, T_n))$, C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), 397–402.
- [7] A. Weil, Basic Number Theory, 3rd ed., Grundlehren Math. Wiss. 144, Springer, 1974.

L.A.T.P.–U.M.R. 6632 Bâtiment Henri Poincaré Faculté des Sciences de St-Jérôme Av. Escadrille Normandie Niemen 13397 Marseille Cedex 20, France E-mail: mireille.car@univ.u-3mrs.fr

> Received on 6.11.2002 and in revised form on 24.9.2003

(4395)