Let \( \mathbb{F}_q \) be a finite field of \( q \) elements. E. Howe has shown that there is a natural correspondence between the isogeny classes of two-dimensional ordinary abelian varieties over \( \mathbb{F}_q \) which do not contain a principally polarized variety and pairs of positive integers \((a, b)\) satisfying \( q = a^2 + b \), where \( \gcd(q, b) = 1 \) and all prime divisors \( \ell \) of \( b \) are in the arithmetic progression \( \ell \equiv 1 \pmod{3} \). This arithmetic criterion allows us to give good upper bounds, and for many finite fields good lower bounds, for the frequency of occurrence of isogeny classes of varieties having this property.

1. Introduction

Let \( q \) be a prime power and let \( \mathbb{F}_q \) be a finite field of \( q \) elements. E. Howe [12, Theorem 1.3] has shown that there is a bijection between isogeny classes of two-dimensional ordinary abelian varieties over \( \mathbb{F}_q \) that do not contain a principally polarized variety and pairs of positive integers \((a, b)\) satisfying

\[
q = a^2 + b
\]

with \( \gcd(q, b) = 1 \) and such that all prime divisors \( \ell \) of \( b \) are in the arithmetic progression \( \ell \equiv 1 \pmod{3} \). Thus, we define \( f(q) \) as the number of representations (1) with such integers \( a \) and \( b \). We recall that a \( g \)-dimensional abelian variety over \( \mathbb{F}_q \) (where \( q \) is a power of the prime \( p \)) is ordinary if it has, over an algebraic closure, exactly \( p^g \) points of order dividing \( p \). See [12, Definition 3.1] for this and several other equivalent characterizations of ordinary varieties.

One may use sieve methods, as in Section 14.8 of [10], to sieve the sequence

\[
\{ q - a^2 : 1 \leq a \leq q^{1/2}\},
\]
say, by those primes \( p \leq q^{1/3} \) with \( p \not\equiv 1 \pmod{3} \). One obtains, essentially by Brun’s sieve, an upper bound for \( f(q) \), namely:

**Theorem 1.** For all primes \( q \geq 5 \) we have

\[
f(q) = O \left( C(q) \sqrt{q/ \log q} \right),
\]

where

\[
C(q) = \prod_{p \leq q^{1/3}} \left( 1 - \frac{\chi_4(p)}{p} \right)^{1/2} \left( 1 - \frac{\chi_{-3q}(p)}{p} \right)^{-1/2}
\]

and \( \chi_D \) denotes the real Dirichlet character of conductor \( D \).
The proof, which we do not give, is almost identical to the proof of Bound (14.79) in [10]. We remark that an only slightly more complicated bound holds in the case of general integers $q$, but, because of our motivating application and since it also simplifies some statements, we restrict throughout the paper to the case of $q$ being prime.

The bound of Theorem 1 is presumably tight up to multiplication by a positive absolute constant. However, the function $C(q)$ is not so well understood. Clearly, by Mertens’ theorem (see for example [13, Equation (2.16)]),

$$C_1 (\log q)^{-1} \leq C(q) \leq C_2 \log q$$

for some absolute constants $C_1, C_2 > 0$. However, no tighter bound taking into account the cancellations between the values of the characters in (2) is known. Thus, based on what is currently available, $C(q)$ could conceivably vary with $q$ up to a factor of $(\log q)^{\pm 1}$ and it certainly does vary with $q$ up to some factor which is a power of $\log \log q$.

If one assumes the Riemann Hypothesis for the Dirichlet $L$-functions $L(s, \chi_D)$ with $D = q$ and $D = -3q$, then the products in (2) may be completed so that the bound of Theorem 1 holds with

$$C(q) = L(1, \chi_{-3q})^{1/2} L(1, \chi_q)^{-1/2}$$

and the variation in the values of $C(q)$ with $q$ is known, under these hypotheses, to be by a factor of no more than $(\log \log q)^{\pm 1}$.

One could try to approach the lower bound using the same tool, the semi-linear sieve, which yields the upper bound, and one would expect it to provide a lower bound of order matching the upper bound in Theorem 1. In the case of a quadratic polynomial, just for example the sequence $q + a^2$, with $q$ fixed and $1 \leq a \leq A$, $A$ large, the sieve does succeed [9] in obtaining the expected lower bound of order $A/\sqrt{\log A}$ (provided in this case that $q$ is any integer with $q \not\equiv 2 \pmod{3}$). However, that bound depends in an unspecified way on the coefficients of the polynomial. In our case, the coefficient $q$ is large and success with the sieve awaits the development of analytic input stronger than what is currently available. We expect, although we did not check every detail, that the more recent and deeper arguments of [10, Section 14.8] as completed in [8] would give a lower bound matching the upper bound, that is,

$$f(q) \geq C_0 L(1, \chi_{-3q})^{1/2} L(1, \chi_q)^{-1/2} \sqrt{q/\log q},$$

for some absolute constant $C_0 > 0$, but only subject to the assumption of the same two instances of the Riemann Hypothesis.

As our main result, we obtain a lower bound which comes close to the right order and is not based on any unproved assumptions.

**Theorem 2.** For primes $q \equiv 11 \pmod{12}$, we have

$$f(q) \geq q^{1/2 + o(1)}.$$

We remark that, although the factor $q^{o(1)}$ might look a little on the weak side, in fact, even if one were given the bound (4) as a black box, one could do no better with it than [5], based on current unconditional bounds for $L$-functions (Siegel’s theorem).

It is interesting to compare the bounds of Theorems 1 and 2 with the well-known fact that the number $O(q)$ of isogeny classes of two-dimensional ordinary abelian
varieties are far more numerous, satisfying $cq^{3/2} \leq \mathcal{O}(q) \leq Cq^{3/2}$ for two absolute constants $C > c > 0$. See [6, Theorem 1.2] for a much more general and precise (asymptotic) result.

2. Our approach

To prove our theorem, we appeal, instead of the above, to the theory of ternary quadratic forms. As usual in dealing with the representation of integers by such forms, only certain congruence classes are eligible.

We note that if a prime $p > 3$ divides $4y^2 + 3z^2$ for an arbitrary integer $y$ and an odd integer $z$, then unless $p \mid z$ (and thus also $p \mid y$), we have

$$\left(\frac{-3}{p}\right) = 1,$$

where $(m/p)$ denotes the Legendre symbol of $m$ modulo $p$ and therefore $p \equiv 1 \pmod{3}$.

We also note that if an odd prime $q \equiv 2 \pmod{3}$ is represented by the integral ternary form $q = 4x^2 + 4y^2 + 3z^2$, then $z$ is odd and

$$\gcd(4y^2 + 3z^2, 6) = 1,$$

as otherwise either $q \equiv 4x^2 \equiv 0, 1 \pmod{3}$ or $q \equiv 0 \pmod{2}$.

Since every positive integer $b$ has at most $b^{o(1)}$ representations by the integral binary form $b = 4y^2 + 3z^2$ (it is bounded by the number of ideals of norm $b$ in the ring of integers of the field $\mathbb{Q}(\sqrt{-3})$), we see that for $q \equiv 2 \pmod{3}$ we have

$$f(q) \geq q^{o(1)}R(q),$$

where $R(n)$ is the number of representations of the integer $n$ by the ternary form

$$F_1(x, y, z) = 4x^2 + 4y^2 + 3z^2$$

with integers $y$ and $z$ such that $\gcd(y, z)$ is not divisible by a prime $p \equiv 2 \pmod{3}$.

Now, let $\mathcal{D}$ denote the set of squarefree positive integers $d$ that are composed only out of the odd primes $p \equiv 2 \pmod{3}$. Therefore, using as usual $\mu(d)$ to denote the Möbius function and recalling (6), (7), by the standard inclusion-exclusion principle we obtain

$$R(q) = \sum_{d \in \mathcal{D}} \mu(d)r_d(q),$$

where $r_d(n)$ is the number of representations of the integer $n = F_d(x, y, z)$ by the ternary form

$$F_d(x, y, z) = 4x^2 + 4d^2y^2 + 3d^2z^2$$

with arbitrary integers $x, y, z$.

We use some ideas of Blomer and Brüdern [3] to relate the values of $r_d(q)$ to the value of

$$r(q) = r_1(q),$$

provided that $d$ is not too large.

We note that the form $F_1(x, y, z)$ has been studied by Dickson [5, Equation (23)]], who showed in particular that the primes represented by the form are just those congruent to three modulo four.

The method of this paper can certainly be modified to apply to other finite fields, for example some higher prime powers. Of greater interest perhaps would be to use...
other ternary forms to extend the result to other prime fields. For example, if one replaces the form (9) by the form
\[ G_1(x, y, z) = 36x^2 + 12y^2 + z^2, \]
then the same arguments apply to show that the lower bound of Theorem 2 holds also as \( q \) runs through the primes \( q \equiv 1 \pmod{3} \) which are represented by \( G_1 \). We expect that the set of primes represented by \( G_1 \) consists of just those congruent to one modulo twelve.

3. Representations by ternary forms

Here we collect some general facts about the representations of integers by a ternary quadratic form; we refer to [14] for background. Most of the results hold in greater generality, but we present them in a way tailored to our applications.

Given a ternary quadratic form
\[ F(x, y, z) = Ax^2 + By^2 + Cz^2 \]
with the determinant \( \Delta = 8ABC \neq 0 \) (here we follow the modern notation as in [2] or [7], as opposed to Siegel [15], who would have suppressed the factor 8), we denote
\[ r(F, n) = \# \{(x, y, z) \in \mathbb{Z}^3 : F(x, y, z) = n\} . \]

To formulate the necessary asymptotic results about the behavior of \( r(F, n) \) we need to introduce more notation. For integers \( m \) and \( n \) we denote by \( N_F(m, n) \) the number of solutions to the congruence
\[ F(x, y, z) \equiv n \pmod{m}, \quad 0 \leq x, y, z < m. \]

For a prime \( p \), we define the \( p \)-adic density
\[ \chi_F(p, n) = \lim_{k \to \infty} \frac{N_F(p^k, n)}{p^{2k}}, \]
where \( k \) runs through positive integers. The existence of the limit follows from a classical result of Siegel [15, Hilfsatz 13], which in fact shows that the ratio \( N_F(p^k, n)/p^{2k} \) eventually stabilizes. We present it in a very special case that is relevant to our current needs:

Lemma 3. For any primes \( p \) and \( q \) with \( p \nmid 2q \) we have
\[ \chi_F(p, q) = \frac{N_F(p, q)}{p^2} . \]

Furthermore, by [15, Hilfsatz 12] (or see also [2, Section 1.1]) we have:

Lemma 4. For a prime \( p \) with \( p \nmid 2nABC \) we have
\[ \chi_F(p, n) = 1 + \frac{1}{p} \left( \frac{-nABC}{p} \right). \]

We next define the singular series
\[ \mathcal{G}_F(n) = \prod_{p \text{ prime}} \chi_F(p, n) \]
which, by the formula for \( \chi_F \), conditionally converges. (It is essentially the \( L \)-function at \( s = 1 \); see also [2, Section 1.1].)
We are now able to formulate our main technical tool:

**Lemma 5.** For any ternary quadratic form (12) and squarefree \( n \), we have

\[
r(F,n) = r(\text{gen } F,n) + O(ABCn^{13/28+o(1)}),
\]

where

\[
r(\text{gen } F,n) = \frac{2\pi}{\sqrt{ABC}}S_F(n)n^{1/2},
\]

uniformly in \( A, B \) and \( C \).

**Proof.** By a result of Blomer [1, Theorem 1], for squarefree \( n \) we have

\[
r(F,n) = r(\text{spn } F,n) + O(ABCn^{13/28+o(1)}),
\]

where \( r(\text{spn } F,n) \) is a certain weighted average number of representations of \( n \) by all ternary forms in the spinor genus of \( F \); see [2, Equation (1.5)].

Furthermore, since \( n \) is squarefree we have

\[
r(\text{spn } F,n) = r(\text{gen } F,n);
\]

see, for example, [2, Section 1.2, p. 4], where several sufficient conditions for (14) are given, including the squarefreeness of \( n \). Finally, we recall [13, Theorem 20.15], which gives an explicit formula for the “expected value” \( r(\text{gen } F,n) \).

\[\square\]

4. **Asymptotic Formula for** \( r_d(q) \)

From now on we work with the ternary forms of specific interest to us. We define

\[
\mathcal{S}(d,n) = \mathcal{S}_{F_d}(n) \quad \text{and} \quad \chi(d,p,n) = \chi_{F_d}(p,n),
\]

where \( F_d(x,y,z) \) is given by (11), and set

\[
\mathcal{S}(n) = \mathcal{S}(1,n).
\]

Following an idea of Blomer and Brüdern [3] we also define

\[
\omega(d,n) = \frac{\mathcal{S}(d,n)}{\mathcal{S}(n)}.
\]

We note that if \( p \nmid d \) and the form \( F_d \) is given by (11), then, after the change of variables \( x \to x, dy \to y, z \to z \), we see that \( N_{F_d}(p^k,n) = N_{F_1}(p^k,n) \)

for \( k = 1, 2, \ldots \).

Thus we obtain the following explicit formula (see also [3, Section 3]).

**Lemma 6.** For any integers \( n \geq 1 \) and \( d \in \mathcal{D} \), we have

\[
\omega(d,n) = \prod_{p\mid d} \omega(d,p,n),
\]

where

\[
\omega(d,p,n) = \frac{\chi(d,p,n)}{\chi(p,n)}.
\]

We now evaluate the \( p \)-adic densities \( \chi(d,p,n) \) for \( p \mid d \). As before, for a prime \( p \geq 3 \) and an integer \( n \), we use \( (n/p) \) to denote the Legendre symbol of \( n \) modulo \( p \).

**Lemma 7.** For any prime \( q \) and \( d \in \mathcal{D} \) and a prime \( p \neq q \) with \( p \mid d \), we have

\[
\chi(d,p,q) = 1 + \left( \frac{q}{p} \right).
\]
Proof. For \( p | d \) we have
\[
N_{F_d}(p, q) = p^2 \left( 1 + \left( \frac{q}{p} \right) \right).
\]
The result now follows immediately from Lemma 3. \( \square \)

**Lemma 8.** For an odd prime \( q \equiv 2 \pmod{3} \) and \( d \in \mathcal{D} \) with \( d < q \) we have
\[
\omega(d, q) = \prod_{p|d} \frac{1 + \left( \frac{q}{p} \right)}{1 - \left( \frac{q}{p} \right) p^{-1}}.
\]

Proof. Using Lemmas 7 and 4 we obtain
\[
\omega(d, q) = \prod_{p|d} \frac{1 + \left( \frac{q}{p} \right)}{1 + \left( \frac{-3q}{p} \right) p^{-1}}.
\]
It now remains to recall the multiplicativity of the Legendre symbol and that
\[
\left( \frac{-3}{p} \right) = -1
\]
for \( p \equiv 2 \pmod{3} \). \( \square \)

We now use \( \mathcal{D}_q \) to denote the set of \( d \in \mathcal{D} \) such that we have
\[
\left( \frac{q}{p} \right) = 1
\]
for every prime divisor \( p | d \). In particular, we see from Lemma 8 that (10) can be written as
\[
(15) \quad R(q) = \sum_{d \in \mathcal{D}_q} \mu(d) r_d(q).
\]
Combining Lemma 5 and Lemma 8 we derive the desired asymptotic formula for \( r_d(q) \):

**Lemma 9.** For an odd prime \( q \equiv 2 \pmod{3} \) and \( d \in \mathcal{D}_q \), we have
\[
r_d(q) = \frac{\pi}{2\sqrt{3}} \frac{\eta(d)}{d^2} \mathcal{S}(q) q^{1/2} + O(d^{4/3} q^{13/28+o(1)}).
\]
where
\[
\eta(d) = \prod_{p|d} \frac{2p}{p - 1}.
\]

5. **Upper bound for** \( r_d(q) \)

For large values of \( d \), when Lemma 9 is of no use, we apply the following upper bound.

**Lemma 10.** For any integers \( n \) and \( d \) with \( \gcd(n, d) = 1 \) and \( 1 \leq d \leq n^{1/2} \), we have
\[
r_d(n) \leq (n^{1/2} d^{-2} + 1)n^{o(1)}.
\]
Proof. We note that for every integer solution to the equation $F_d(x, y, z) = n$ we have $4x^2 \equiv n \pmod{d^2}$. When $d$ is fixed with $\gcd(n, d) = 1$ (in fewer than $n^{1/2}$ possible ways), there are no more than $\varphi(d) \leq n^{o(1)}$ solutions to this congruence and hence no more than $(n^{1/2}d^{-2} + 1)n^{o(1)}$ integers $|x| \leq n^{1/2}$ which satisfy it. Once $x$ is also fixed, so is $4y^2 + 3z^2$, and then the number of choices of $y$ and $z$ is bounded by the number of ideals of that norm in the ring of integers of the field $\mathbb{Q}(\sqrt{-3})$ which as before is bounded by $n^{o(1)}$. □

6. Singular series

We note that, by classical bounds for $L$-functions at $s = 1$, we have an upper bound and also, if $\mathcal{G}(q) > 0$, then a lower bound, both of the form

$$\mathcal{G}(q) = q^{o(1)};$$

see also [13, Section 20.4].

Furthermore, to prove that $\mathcal{G}(q) > 0$, because the product converges it is enough to show that none of the local factors vanishes. Actually, by Siegel [15] (see for example [7, Equation (4)]) it is enough to show that the specific congruence

$$q \equiv 4x^2 + 4y^2 + 3z^2 \pmod{(2\Delta)^3}$$

is solvable, where

$$\Delta = \left( \frac{\partial^2 F_1}{\partial x_i \partial x_j} \right)_{i,j=1}^3 = 2^7 \cdot 3$$

is the determinant of the quadratic form $F_1(x_1, x_2, x_3) = 4x_1^2 + 4x_2^2 + 3x_3^2$.

In turn, for primes $q \equiv 3 \pmod{4}$ this follows immediately from the result of Dickson [5, Equation (23)] who showed that there are always global solutions; thus

$$\mathcal{G}(q) > 0.$$

7. Concluding the proof

We now choose a parameter $D \geq 1$ and use Lemma 9 for $d \leq D$ and Lemma 10 for $d > D$. Then from (15) we derive

$$R(q) = \frac{\pi}{2\sqrt{3}} \mathcal{G}(q)q^{1/2} \sum_{\substack{d \in \mathcal{D}_q \\ d \leq D}} \mu(d) \frac{\eta(d)}{d^2} + O \left( D^5 q^{13/28 + o(1)} + D^{-1} q^{1/2 + o(1)} \right).$$

Clearly we have

$$\eta(d) = 2^{\omega(d)} \frac{d}{\varphi(d)},$$

where $\omega(d)$ is the number of distinct prime divisors and $\varphi(d)$ is the Euler function of $d$. Thus, using the well-known bounds for $\omega(d)$ and $\varphi(d)$ (see [11, Theorems 317 and 328]), we derive $\eta(d) \leq d^{o(1)}$. Therefore

$$\sum_{\substack{d \in \mathcal{D}_q \\ d \leq D}} \mu(d) \frac{\eta(d)}{d^2} = \sum_{d \in \mathcal{D}_q} \mu(d) \frac{\eta(d)}{d^2} + O(D^{-1 + o(1)}) = \rho(q) + O(D^{-1 + o(1)}),$$

where

$$\rho(q) = \prod_{p \in \mathcal{D}_q} \left( 1 - \frac{2}{p(p-1)} \right).$$
We note that
\[(20) \quad 1 \geq \rho(q) \geq \prod_{p \equiv 2 \pmod{3}} \left( 1 - \frac{2}{\rho(p-1)} \right).\]

Substituting (19) in (18), and using (16) and (20), we derive
\[R(q) = \frac{\pi}{2\sqrt{3}} \rho(q) \mathbb{E}(q) q^{1/2} + O \left( D^5 q^{13/28 + o(1)} + D^{-1} q^{1/2 + o(1)} \right).\]

Taking \(D = q^{1/168}\) yields
\[(21) \quad R(q) = \frac{\pi}{2\sqrt{3}} \rho(q) \mathbb{E}(q) q^{1/2} + O \left( q^{83/168 + o(1)} \right).\]

Recalling (8), (16), (17) and (20), we see that (21) implies the desired result.

**Acknowledgments**

This work started during a very enjoyable visit of the second author to the University of Toronto. The support and hospitality of this institution is gratefully acknowledged. During the preparation of this paper, the first author was supported in part by NSERC Grant A5123, and the second author by ARC Grant DP1092835.

The authors thank the referee for some useful suggestions which improved the exposition in the paper.

**References**


Department of Mathematics, University of Toronto, Toronto, Ontario M5S 2E4, Canada

E-mail address: frdelndr@math.toronto.edu

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: igor@ics.mq.edu.au