Small solutions of quadratic congruences

Stephan Baier

RKMVERI

June 29, 2022

Quadratic forms representing 0

- Let $Q(x_1, \ldots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and assume $(x_1, \ldots, x_n) \in \mathbb{Z}^n$.

Quadratic forms representing 0

- Let $Q(x_1, \ldots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and assume $(x_1, \ldots, x_n) \in \mathbb{Z}^n$.
- Questions about integer representations by quadratic forms have a long history. There is an abundance of results.

Quadratic forms representing 0

- Let $Q(x_1, \dots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and assume $(x_1, \dots, x_n) \in \mathbb{Z}^n$.
- Questions about integer representations by quadratic forms have a long history. There is an abundance of results.
- A famous theorem by Meyer states that if $n \ge 5$ and Q is indefinite and non-degenerate, then Q represents 0 non-trivially.

Quadratic forms representing 0

- Let $Q(x_1, \dots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and assume $(x_1, \dots, x_n) \in \mathbb{Z}^n$.
- Questions about integer representations by quadratic forms have a long history. There is an abundance of results.
- A famous theorem by Meyer states that if $n \geq 5$ and Q is indefinite and non-degenerate, then Q represents 0 non-trivially.
- If Q has real coefficients and is not a multiple of a form with rational coefficients and is indefinite and non-degenerate, then the Oppenheim conjecture proposes that the set of values is dense in $\mathbb{R}$ as $(x_1, \dots, x_n)$ runs over $\mathbb{Z}^n$, provided that $n \geq 3$.

Quadratic forms representing 0

- Let $Q(x_1, \ldots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and assume $(x_1, \ldots, x_n) \in \mathbb{Z}^n$.
- Questions about integer representations by quadratic forms have a long history. There is an abundance of results.
- A famous theorem by Meyer states that if $n \ge 5$ and Q is indefinite and non-degenerate, then Q represents 0 non-trivially.
- If Q has real coefficients and is not a multiple of a form with rational coefficients and is indefinite and non-degenerate, then the Oppenheim conjecture proposes that the set of values is dense in $\mathbb{R}$ as $(x_1, \ldots, x_n)$ runs over $\mathbb{Z}^n$, provided that $n \ge 3$.
- This was famously proved by Margulis using ergodic theory.

Quadratic congruences representing 0

- It is also interesting to investigate non-trivial representations of 0 in $\mathbb{Z}/q\mathbb{Z}$.

Quadratic congruences representing 0

- It is also interesting to investigate non-trivial representations of 0 in $\mathbb{Z}/q\mathbb{Z}$.
- Here one is mainly interested in *small* non-zero solutions $(x_1, ..., x_n)$.

Quadratic congruences representing 0

- It is also interesting to investigate non-trivial representations of 0 in $\mathbb{Z}/q\mathbb{Z}$.
- Here one is mainly interested in *small* non-zero solutions $(x_1, ..., x_n)$.
- So the question becomes: Given a modulus q, how large does one need to choose N to guarantee the existence of non-zero solutions of the congruence

$$Q(x_1, ..., x_n) \equiv 0 \bmod q$$

with $\max\{|x_1|, ..., |x_n|\} \leq N$? Moreover, how do the solutions distribute?

Quadratic congruences representing 0

- It is also interesting to investigate non-trivial representations of 0 in $\mathbb{Z}/q\mathbb{Z}$.
- Here one is mainly interested in *small* non-zero solutions $(x_1, ..., x_n)$.
- So the question becomes: Given a modulus q, how large does one need to choose N to guarantee the existence of non-zero solutions of the congruence

$$Q(x_1, ..., x_n) \equiv 0 \bmod q$$

  with $\max\{|x_1|, ..., |x_n|\} \leq N$? Moreover, how do the solutions distribute?
- These problems have received a lot of attention as well. Particularly interesting is the case when $n = 3$.

Some history of the problem

- Schinzel, Schlickewei and Schmidt [1]: There is a non-zero solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $\max\{|x_1|, |x_2|, |x_3|\} = O(q^{2/3})$, where the O-constant is absolute.

Some history of the problem

- Schinzel, Schlickewei and Schmidt [1]: There is a non-zero solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $\max\{|x_1|, |x_2|, |x_3|\} = O(q^{2/3})$, where the O-constant is absolute.
- Heath-Brown [4]: The exponent $2/3$ can be replaced by $3/5 + \varepsilon$ if $(\det Q, q) = 1$ and q odd and square-free.

Some history of the problem

- Schinzel, Schlickewei and Schmidt [1]: There is a non-zero solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $\max\{|x_1|, |x_2|, |x_3|\} = O(q^{2/3})$, where the O-constant is absolute.
- Heath-Brown [4]: The exponent $2/3$ can be replaced by $3/5 + \varepsilon$ if $(\det Q, q) = 1$ and q odd and square-free.
- Cochrane [4]: If Q is *fixed*, then $2/3$ can be replaced by $1/2$.

Some history of the problem

- Schinzel, Schlickewei and Schmidt [1]: There is a non-zero solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $\max\{|x_1|, |x_2|, |x_3|\} = O(q^{2/3})$, where the O-constant is absolute.
- Heath-Brown [4]: The exponent $2/3$ can be replaced by $3/5 + \varepsilon$ if $(\det Q, q) = 1$ and q odd and square-free.
- Cochrane [4]: If Q is *fixed*, then $2/3$ can be replaced by $1/2$.
- Hakimi [1]: He focused on prime power moduli $q = p^n$ and made progress on quadratic forms with a large number k of variables.

Our work

- My PhD student Anup Haldar and I [1] recently studied the *asymptotic behavior* of small solutions of diagonal quadratic congruences

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 \equiv 0 \bmod q$$

with $(x_1x_2x_3, q) = 1$ if $q = p^n$ is a power of a fixed odd prime p. We also assumed $(\alpha_1\alpha_2\alpha_3, p) = 1$.

Our work

- My PhD student Anup Haldar and I [1] recently studied the *asymptotic behavior* of small solutions of diagonal quadratic congruences

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 \equiv 0 \bmod q$$

  with $(x_1x_2x_3, q) = 1$ if $q = p^n$ is a power of a fixed odd prime p. We also assumed $(\alpha_1\alpha_2\alpha_3, p) = 1$.
- As pointed out by Heath-Brown [4], the existence of *non-zero* solutions $\ll q^\theta$ for *all* odd moduli follows if one has established it for all *square-free* odd moduli: If $q = q_0^2 q_1$ with q_1 square-free and $Q(x_1, x_2, x_3) \equiv 0 \bmod q_1$, then $Q(q_0x_1, q_0x_2, q_0x_3) \equiv 0 \bmod q$. However, if we restrict ourselves to solutions satisfying $(x_1x_2x_3, q) = 1$, then this argument does not work any longer since q_0 is itself a power of p if $q = p^n$.

Our main results

Theorem

Let $\varepsilon > 0$ be fixed, $p > 5$ be a fixed prime and $\alpha_1, \alpha_2, \alpha_3$ be fixed integers which are coprime to p. Let $\Phi : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be a Schwartz class function. Set $q := p^n$. Then as $n \to \infty$, we have an asymptotic formula of the form

$$\sum_{\substack{(x_1,x_2,x_3)\in\mathbb{Z}^3 \\ (x_1x_2x_3,p)=1 \\ \alpha_1x_1^2+\alpha_2x_2^2+\alpha_3x_3^2\equiv 0 \bmod q}} \Phi\left(\frac{x_1}{N}\right)\Phi\left(\frac{x_2}{N}\right)\Phi\left(\frac{x_3}{N}\right) \sim \hat{\Phi}(0)^3 \cdot C_p \cdot \frac{N^3}{q},$$

provided that $N \geq q^{1/2+\varepsilon}$.

Our main results

In the above theorem,

$$C_p = C_p(\alpha_1, \alpha_2, \alpha_3) := \frac{(p - s_p(\alpha_1, \alpha_2, \alpha_3))(p-1)}{p^2}$$

and

$$s_p(\alpha_1, \alpha_2, \alpha_3) := 2 + \left(\frac{-\alpha_1\alpha_2}{p}\right) + \left(\frac{-\alpha_1\alpha_3}{p}\right) + \left(\frac{-\alpha_2\alpha_3}{p}\right).$$

Moreover, we have the following:

Theorem

Let the conditions in Theorem 1 be kept except that $\alpha_1, \alpha_2, \alpha_3$ are no longer fixed but allowed to vary with n. Then the asymptotic formula above holds if $N \geq q^{11/18+\varepsilon}$.

Our main results

Corollary

Let $\varepsilon > 0$ be fixed and $p > 5$ be a fixed prime. Set $q := p^n$. For $\alpha_1, \alpha_2, \alpha_3$ let $m(\alpha_1, \alpha_2, \alpha_3; q)$ be the smallest value of $\max\{|x_1|, |x_2|, |x_3|\}$ such that $(x_1x_2x_3, p) = 1$ and (x_1, x_2, x_3) is a solution of the congruence in question. Then:

(i) If $\alpha_1, \alpha_2, \alpha_3$ are fixed and satisfy $(\alpha_1\alpha_2\alpha_3, p) = 1$, then, as $n \to \infty$, we have

$$m(\alpha_1, \alpha_2, \alpha_3; q) \ll_{\alpha_1,\alpha_2,\alpha_3,p,\varepsilon} q^{1/2+\varepsilon}.$$

(ii) As $n \to \infty$, we have

$$\max_{\substack{\alpha_1,\alpha_2,\alpha_3 \bmod q \\ (\alpha_1\alpha_2\alpha_3,p)=1}} m(\alpha_1, \alpha_2, \alpha_3; q) \ll_{p,\varepsilon} q^{11/18+\varepsilon}.$$

Connection with the Oppenheim conjecture

- Quantitative versions of the Oppenheim conjecture establish the existence of solutions $(x_1, ..., x_n)$ of

$$|Q(x_1, ..., x_n) - \sigma| < \delta$$

for $\max\{|x_1|, ..., |x_n|\} \leq N(\delta)$. A particular case is that of $\sigma = 0$ (good approximations of zero).

Connection with the Oppenheim conjecture

- Quantitative versions of the Oppenheim conjecture establish the existence of solutions $(x_1, ..., x_n)$ of

$$|Q(x_1, ..., x_n) - \sigma| < \delta$$

for $\max\{|x_1|, ..., |x_n|\} \leq N(\delta)$. A particular case is that of $\sigma = 0$ (good approximations of zero).
- A quantitative version of the Oppenheim conjecture was established for $\sigma = 0$ and $n = 5$ by Davenport and Heilbronn [2] using a variant of the circle method.

Connection with the Oppenheim conjecture

- Quantitative versions of the Oppenheim conjecture establish the existence of solutions $(x_1, \ldots, x_n)$ of

$$|Q(x_1, \ldots, x_n) - \sigma| < \delta$$

for $\max\{|x_1|, \ldots, |x_n|\} \leq N(\delta)$. A particular case is that of $\sigma = 0$ (good approximations of zero).

- A quantitative version of the Oppenheim conjecture was established for $\sigma = 0$ and $n = 5$ by Davenport and Heilbronn [2] using a variant of the circle method.
- Our results may be viewed as p-adic versions of these results: We seek to find solutions $(x_1, \ldots, x_n)$ of $|Q(x_1, \ldots, x_n)|_p < \delta$ for $\max\{|x_1|, \ldots, |x_n|\} \leq N(\delta)$.

Pythagorean triples modulo prime powers

- A particular case is when $\alpha_1, \alpha_2 = 1$ and $\alpha_3 = -1$.

Pythagorean triples modulo prime powers

- A particular case is when $\alpha_1, \alpha_2 = 1$ and $\alpha_3 = -1$.
- In this case, our congruence takes the form

$$x_1^2 + x_2^2 \equiv x_3^2 \bmod q.$$

Pythagorean triples modulo prime powers

- A particular case is when $\alpha_1, \alpha_2 = 1$ and $\alpha_3 = -1$.
- In this case, our congruence takes the form

$$x_1^2 + x_2^2 \equiv x_3^2 \bmod q.$$

- This is the case of Pythagorean triples modulo prime powers.

Pythagorean triples modulo prime powers

- A particular case is when $\alpha_1, \alpha_2 = 1$ and $\alpha_3 = -1$.
- In this case, our congruence takes the form

$$x_1^2 + x_2^2 \equiv x_3^2 \bmod q.$$

- This is the case of Pythagorean triples modulo prime powers.
- If $\max\{|x_1|, |x_2|, |x_2|\} \leq N < \sqrt{q/2}$, then these are ordinary Pythagorean triples, i.e.

$$x_1^2 + x_2^2 \equiv x_3^2.$$

In this case, we have a different asymptotic of the form $\sim D_p N \log N$.

Pythagorean triples modulo prime powers

- A particular case is when $\alpha_1, \alpha_2 = 1$ and $\alpha_3 = -1$.
- In this case, our congruence takes the form

$$x_1^2 + x_2^2 \equiv x_3^2 \bmod q.$$

- This is the case of Pythagorean triples modulo prime powers.
- If $\max\{|x_1|, |x_2|, |x_2|\} \leq N < \sqrt{q/2}$, then these are ordinary Pythagorean triples, i.e.

$$x_1^2 + x_2^2 \equiv x_3^2.$$

  In this case, we have a different asymptotic of the form $\sim D_p N \log N$.
- It is best to illustrate our method by looking at this particular case. In fact, we worked out this case first (see [2]).

Parametrization of points

- Our congruence resembles the equation

$$x_1^2 + x_2^2 - x_3^2 = 0$$

of a circle in homogeneous coordinates. Indeed, every solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ with $(x_1x_2x_3, p) = 1$ of this congruence comes from a solution of the above circle equation in the p-adic integers. This can be seen by a Hensel type argument.

Parametrization of points

- Our congruence resembles the equation

$$x_1^2 + x_2^2 - x_3^2 = 0$$

  of a circle in homogeneous coordinates. Indeed, every solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$ with $(x_1 x_2 x_3, p) = 1$ of this congruence comes from a solution of the above circle equation in the p-adic integers. This can be seen by a Hensel type argument.
- In affine coordinates, the circle equation takes the form

$$y_1^2 + y_2^2 - 1 = 0.$$

Parametrization of points

- Using a well-known parametrization of K-rational points of the unit circle (in this case, take $K := \mathbb{Q}_p$) , the solutions (y_1, y_2) with $(y_1 y_2, p) = 1$ of the congruence

$$y_1^2 + y_2^2 - 1 \equiv 0 \bmod p^n$$

are parametrized in the form

$$y_1 = \frac{1-t^2}{1+t^2}, \quad y_2 = \frac{2t}{1+t^2}, \quad t \bmod p^n$$

with

$$\gcd\left(t(1-t^2)(1+t^2), p\right) = 1.$$

Here $1/(1+t^2)$ is a multiplicative inverse of $1+t^2$ modulo p^n.

Rewriting the quantity in question

- We now rewrite the quantity in question in the form

$$T = \sum_{(x_3,p)=1} \Phi\left(\frac{x_3}{N}\right) \sum_{\substack{y_1,y_2 \bmod p^n \\ (y_1 y_2,p)=1 \\ y_1^2+y_2^2-1\equiv 0 \bmod p^n}} \sum_{\substack{x_1\equiv x_3 y_1 \bmod p^n \\ x_2\equiv x_3 y_2 \bmod p^n}} \Phi\left(\frac{x_1}{N}\right)\Phi\left(\frac{x_2}{N}\right).$$

Rewriting the quantity in question

- We now rewrite the quantity in question in the form

$$T = \sum_{(x_3,p)=1} \Phi\left(\frac{x_3}{N}\right) \sum_{\substack{y_1,y_2 \bmod p^n \\ (y_1y_2,p)=1 \\ y_1^2+y_2^2-1\equiv 0 \bmod p^n}} \sum_{\substack{x_1\equiv x_3y_1 \bmod p^n \\ x_2\equiv x_3y_2 \bmod p^n}} \Phi\left(\frac{x_1}{N}\right)\Phi\left(\frac{x_2}{N}\right).$$

- At this stage, we recall the Poisson summation formula

$$\sum_{m\in\mathbb{Z}} \Psi(m) = \sum_{n\in\mathbb{Z}} \hat{\Psi}(n),$$

where Ψ is a Schwartz class function and $\hat{\Psi}$ its Fourier transform.

Double Poisson summation

- We now perform double Poisson summation in the sums over x_2 and x_3 and use our above parametrization to get

$$T = \frac{N^2}{p^{2n}} \sum_{(x_3,p)=1} \Phi\left(\frac{x_3}{N}\right) \sum_{(k_1,k_2)\in\mathbb{Z}^2} \hat{\Phi}\left(\frac{k_1 N}{p^n}\right) \hat{\Phi}\left(\frac{k_2 N}{p^n}\right) \times$$

$$\sum_{\substack{t \bmod p^n \\ (t(1-t^2)(1+t^2),p)=1}} e_{p^n}\left(x_3 \cdot \frac{k_1(1-t^2)+2k_2 t}{1+t^2}\right),$$

where $e_q(z) := e^{2\pi i z/q}$.

Double Poisson summation

- We now perform double Poisson summation in the sums over x_2 and x_3 and use our above parametrization to get

$$T = \frac{N^2}{p^{2n}} \sum_{(x_3,p)=1} \Phi\left(\frac{x_3}{N}\right) \sum_{(k_1,k_2)\in\mathbb{Z}^2} \hat{\Phi}\left(\frac{k_1 N}{p^n}\right) \hat{\Phi}\left(\frac{k_2 N}{p^n}\right) \times \sum_{\substack{t \bmod p^n \\ (t(1-t^2)(1+t^2),p)=1}} e_{p^n}\left(x_3 \cdot \frac{k_1(1-t^2)+2k_2 t}{1+t^2}\right),$$

  where $e_q(z) := e^{2\pi i z/q}$.
- Nicely, we now have a complete exponential sum to modulus p^n as inner-most sum. This can be evaluated completely using a general theorem by Cochrane and Ziyong [1] on complete exponential sums with rational functions.

Main term contribution

- We decompose T into

$$T = T_0 + U,$$

where T_0 is the main term contribution of $(k_1, k_2) = (0, 0)$.

Main term contribution

- We decompose T into

$$T = T_0 + U,$$

where T_0 is the main term contribution of $(k_1, k_2) = (0, 0)$.

- It is easy to prove that

$$T_0 = \hat{\Phi}(0)^3 \cdot C_p \cdot \frac{N^3}{p^n} \cdot (1 + o(1))$$

as $n \to \infty$.

A dual problem

- It remains to bound the error term U, the contribution of all pairs $(k_1, k_2) \neq (0, 0)$.

A dual problem

- It remains to bound the error term U, the contribution of all pairs $(k_1, k_2) \neq (0,0)$.
- I omit a whole chunk of technical details. After evaluating the said complete exponential sum over t and performing another Poisson summation in x_3, we are down to the following bound.

$$U \ll \frac{N^3}{p^{3n/2}} \sum_{r=0}^{n-2} p^{r/2} \sum_{\substack{(l_1,l_2,l_3)\in\mathbb{Z}^3 \\ (l_1 l_2 l_3,p)=1 \\ |l_1|,|l_2|,|l_3|\le L_r \\ l_1^2+l_2^2\equiv l_3^2 \bmod p^{n-r-1}}} 1 + O_\varepsilon(1),$$

where

$$L_r := p^{n-r+n\varepsilon} N^{-1}.$$

A dual problem

- Now if $L_r < \sqrt{p^{n-r-1}/2}$, then the congruence

$$l_1^2 + l_2^2 \equiv l_3^2 \bmod p^{n-r-1}$$

above can be replaced by the equation

$$l_1^2 + l_2^2 = l_3^2,$$

i.e., (l_1, l_2, l_3) is an ordinary Pythagorean triple. Certainly, this is the case if $N \geq p^{n/2+2n\varepsilon}$ and n is large enough. Hence, in this case, we have

$$U \ll \frac{N^3}{p^{3n/2}} \sum_{r=0}^{n-2} p^{r/2} \sum_{\substack{(l_1,l_2,l_3)\in\mathbb{Z}^3 \\ (l_1 l_2 l_3, p)=1 \\ |l_1|,|l_2|,|l_3|\leq L_r \\ l_1^2+l_2^2=l_3^2}} 1 + O_\varepsilon(1).$$

Completion of the proof

- It is known that the number of Pythagorean triples of height $\leq L$ is bounded by $\ll L \log L$.

Completion of the proof

- It is known that the number of Pythagorean triples of height $\leq L$ is bounded by $\ll L \log L$.
- As a result, we obtain

$$U \ll \frac{N^2}{p^{n/2}} \cdot p^{n\varepsilon} = \frac{N^2}{q^{1/2}} \cdot q^{\varepsilon}.$$

Completion of the proof

- It is known that the number of Pythagorean triples of height $\leq L$ is bounded by $\ll L \log L$.
- As a result, we obtain

$$U \ll \frac{N^2}{p^{n/2}} \cdot p^{n\varepsilon} = \frac{N^2}{q^{1/2}} \cdot q^{\varepsilon}.$$

- This is dominated by the main term of size

$$T_0 \asymp \frac{N^3}{p^n} = \frac{N^3}{q}$$

if $N \geq q^{1/2+2\varepsilon}$, which completes the proof.

General congruences

- Now we want to investigate general congruences.

General congruences

- Now we want to investigate general congruences.
- Let $p > 5$ be a prime and $q = p^n$. We denote the quantity in question as

$$\Sigma_{\alpha_1,\alpha_2,\alpha_3}(\Phi, N, q) := \sum_{\substack{(x_1,x_2,x_3)\in\mathbb{Z}^3 \\ (x_1x_2x_3,p)=1 \\ \alpha_1x_1^2+\alpha_2x_2^2+\alpha_3x_3^2\equiv 0 \bmod q}} \Phi\left(\frac{x_1}{N}\right)\Phi\left(\frac{x_2}{N}\right)\Phi\left(\frac{x_3}{N}\right)$$

In particular, letting $\chi_{[-1,1]}$ be the characteristic function of the interval $[-1,1]$, we have

$$\Sigma_{\alpha_1,\alpha_2,\alpha_3}(\chi_{[-1,1]}, N, q) = \sum_{\substack{|x_1|,|x_2|,|x_3|\le N \\ \alpha_1x_1^2+\alpha_2x_2^2+\alpha_3x_3^3\equiv 0 \bmod q \\ (x_1x_2x_3,q)=1}} 1,$$

which we denote by $\Sigma_{\alpha_1,\alpha_2,\alpha_3}(N, q)$.

General congruences

- Generalizing the above method, we arrive at a formula of the form

$$\Sigma_{\alpha_1,\alpha_2,\alpha_3}(\Phi, N, q) = \Phi(0)^3 \cdot C_p(\alpha_1,\alpha_2,\alpha_3) \cdot \frac{N^3}{q} \cdot (1+o(1)) + O\left(\frac{N^3}{q^{3/2}} \sum_{r=0}^{n-2} p^{r/2} \Sigma_{\beta_1,\beta_2,\beta_3}(L_r, q_r) + O_\varepsilon(1)\right),$$

where

$$L_r := p^{-r} q^{1+\varepsilon} N^{-1}, \quad q_r := p^{-r-1} q,$$

$$\beta_1 := \alpha_2\alpha_3, \quad \beta_2 := \alpha_1\alpha_3, \quad \beta_3 := \alpha_1\alpha_2.$$

General congruences

- Generalizing the above method, we arrive at a formula of the form

$$\Sigma_{\alpha_1,\alpha_2,\alpha_3}(\Phi, N, q) = \Phi(0)^3 \cdot C_p(\alpha_1,\alpha_2,\alpha_3) \cdot \frac{N^3}{q} \cdot (1+o(1)) + O\left(\frac{N^3}{q^{3/2}} \sum_{r=0}^{n-2} p^{r/2} \Sigma_{\beta_1,\beta_2,\beta_3}(L_r, q_r) + O_\varepsilon(1) \right),$$

  where

$$L_r := p^{-r} q^{1+\varepsilon} N^{-1}, \quad q_r := p^{-r-1} q,$$

$$\beta_1 := \alpha_2\alpha_3, \quad \beta_2 := \alpha_1\alpha_3, \quad \beta_3 := \alpha_1\alpha_2.$$

- Now our task is to bound from above the quantity $\Sigma_{\beta_1,\beta_2,\beta_3}(L_r, q_r)$.

Upper bound for the dual problem

- If $\alpha_1, \alpha_2, \alpha_3$ are fixed, a similar argument as before leads to an asymptotic if $N \geq q^{1/2+\varepsilon}$.

Upper bound for the dual problem

- If $\alpha_1, \alpha_2, \alpha_3$ are fixed, a similar argument as before leads to an asymptotic if $N \geq q^{1/2+\varepsilon}$.
- If $\alpha_1, \alpha_2, \alpha_3$ are allowed to vary with n, then this argument fails. We will see in the following what we can do in this case of arbitrary $\alpha_1, \alpha_2, \alpha_3$.

Upper bound for the dual problem

- If $\alpha_1, \alpha_2, \alpha_3$ are fixed, a similar argument as before leads to an asymptotic if $N \geq q^{1/2+\varepsilon}$.
- If $\alpha_1, \alpha_2, \alpha_3$ are allowed to vary with n, then this argument fails. We will see in the following what we can do in this case of arbitrary $\alpha_1, \alpha_2, \alpha_3$.
- It is relatively easy to obtain the bound

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M, q) \ll M^{3/2+\varepsilon}$$

if $M \leq q^{1/2-\varepsilon}$, leading to an asymptotic if $N \geq q^{2/3+\varepsilon}$.

Upper bound for the dual problem

- If $\alpha_1, \alpha_2, \alpha_3$ are fixed, a similar argument as before leads to an asymptotic if $N \geq q^{1/2+\varepsilon}$.
- If $\alpha_1, \alpha_2, \alpha_3$ are allowed to vary with n, then this argument fails. We will see in the following what we can do in this case of arbitrary $\alpha_1, \alpha_2, \alpha_3$.
- It is relatively easy to obtain the bound

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M, q) \ll M^{3/2+\varepsilon}$$

  if $M \leq q^{1/2-\varepsilon}$, leading to an asymptotic if $N \geq q^{2/3+\varepsilon}$.
- Our goal is to beat the exponent $3/2$ above. We shall avoid technical details but just sketch the idea of our method.

Upper bound for the dual problem

- The method depends on the Diophantine properties of the fractions $\beta_1\overline{\beta_3}/q$ and $\beta_2\overline{\beta_3}/q$, where $\overline{\beta_3}$ is a multiplicative inverse modulo q.

Upper bound for the dual problem

- The method depends on the Diophantine properties of the fractions $\beta_1\overline{\beta_3}/q$ and $\beta_2\overline{\beta_3}/q$, where $\overline{\beta_3}$ is a multiplicative inverse modulo q.
- We may write our congruence in the form

$$\beta_1\overline{\beta_3}x_1^2 + \beta_2\overline{\beta_3}x_2^2 \equiv -x_3^2 \bmod q.$$

Upper bound for the dual problem

- The method depends on the Diophantine properties of the fractions $\beta_1\overline{\beta_3}/q$ and $\beta_2\overline{\beta_3}/q$, where $\overline{\beta_3}$ is a multiplicative inverse modulo q.
- We may write our congruence in the form

$$\beta_1\overline{\beta_3}x_1^2 + \beta_2\overline{\beta_3}x_2^2 \equiv -x_3^2 \bmod q.$$

- If both fractions $\beta_1\overline{\beta_3}/q$ and $\beta_2\overline{\beta_3}/q$ have good rational approximations by rational numbers a_1/r_1 and a_2/r_2 with small denominators r_1 and r_2, then we can make the previous argument work, turning from a congruence to an equation of the form

$$\gamma_1 x_1^2 + \gamma_2 x_2^2 = kq - r_1 r_2 x_3^2$$

with γ_1, γ_2, k and $r_1 r_2$ small compared to q and M. For every choice of x_3 and k, the number of solutions to the equation (x_1, x_2) is bounded by $O(M^\varepsilon)$.

Upper bound for the dual problem

- In the complementary case, $\beta_i\overline{\beta_3}$ with $i = 1$ or 2 does not have good approximation by a rational number a/r with small denominator. In this case, we use the Cauchy-Schwarz inequality to reduce the problem to counting solutions (A, B) of the linear congruence $A\beta_i\overline{\beta_3} \equiv B \bmod q$ in a certain box.

Upper bound for the dual problem

- In the complementary case, $\beta_i\overline{\beta_3}$ with $i = 1$ or 2 does not have good approximation by a rational number a/r with small denominator. In this case, we use the Cauchy-Schwarz inequality to reduce the problem to counting solutions (A, B) of the linear congruence $A\beta_i\overline{\beta_3} \equiv B \bmod q$ in a certain box.
- Precisely, we obtain

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M,q)^2 \ll M \left(\Sigma_{\beta_1,\beta_2,\beta_3}(M,q) + M^{\varepsilon} \sum_{\substack{0<|A|,|B|\leq 2M^2 \\ \beta_i\overline{\beta_3}A\equiv B \bmod q}} 1 \right).$$

Upper bound for the dual problem

- Using an earlier result by my PhD student Dwaipayan Mazumder and myself we have a bound of the form

$$\sum_{\substack{0<|A|,|B|\leq 2M^2 \\ \beta_i\overline{\beta_3}A\equiv B \bmod q}} 1 \ll \left(\frac{M^3}{q}+\frac{rM^2}{q}+\frac{M^2}{r}+1\right)(rMq)^{\varepsilon}$$

if

$$\frac{\beta_i\overline{\beta_3}}{q}=\frac{a}{r}+O\left(\frac{1}{r^2}\right).$$

Since r is not small, we obtain a saving over the trivial bound $\ll M^2$.

Upper bound for the dual problem

- Combining both cases, we obtain a bound of the form

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M,q) \ll \left(\frac{M^{5/2}}{q^{1/2}} + \frac{M^{9/5}}{q^{1/5}} + M \right) q^{\varepsilon}$$

if $M \leq q^{1/2-\varepsilon}$. Note that this beats the bound $\ll M^{3/2+\varepsilon}$.

Upper bound for the dual problem

- Combining both cases, we obtain a bound of the form

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M,q) \ll \left(\frac{M^{5/2}}{q^{1/2}} + \frac{M^{9/5}}{q^{1/5}} + M \right) q^{\varepsilon}$$

  if $M \le q^{1/2-\varepsilon}$. Note that this beats the bound $\ll M^{3/2+\varepsilon}$.
- This leads to an asymptotic if $N \ge q^{11/18+\varepsilon}$.

Upper bound for the dual problem

- Combining both cases, we obtain a bound of the form

$$\Sigma_{\beta_1,\beta_2,\beta_3}(M,q) \ll \left(\frac{M^{5/2}}{q^{1/2}} + \frac{M^{9/5}}{q^{1/5}} + M \right) q^{\varepsilon}$$

  if $M \leq q^{1/2-\varepsilon}$. Note that this beats the bound $\ll M^{3/2+\varepsilon}$.

- This leads to an asymptotic if $N \geq q^{11/18+\varepsilon}$.
- A further improvement may be possible by using the circle method (with Kloosterman refinement) to count solutions (x_1, x_2, x_3, k) of the equation

$$\gamma_1 x_1^2 + \gamma_2 x_2^2 + r_1 r_2 x_3^2 = kq.$$

  Recall that $|x_i| \leq M$. The k-range is small compared to M but of significant size. This is subject of current work.

Upper bound for the dual problem

- This leads us to representations by (not necessarily definite) ternary quadratic forms. Ultimately, we encounter Salie sums, which can be evaluated explicitly. These evaluations contain terms of the form $e(hx/c)$, where x is a solution of a quadratic congruence $x^2 \equiv D \bmod c$. Here h is relatively small. Non-trivial estimates for averages over D and c lead to a saving. Work by Duke, Friedlander and Iwaniec [3] obtains a saving for *fixed* D when averaging over the modulus c.

Upper bound for the dual problem

- This leads us to representations by (not necessarily definite) ternary quadratic forms. Ultimately, we encounter Salie sums, which can be evaluated explicitly. These evaluations contain terms of the form $e(hx/c)$, where x is a solution of a quadratic congruence $x^2 \equiv D \bmod c$. Here h is relatively small. Non-trivial estimates for averages over D and c lead to a saving. Work by Duke, Friedlander and Iwaniec [3] obtains a saving for *fixed* D when averaging over the modulus c.
- Note the interesting paper "Small representations by indefinite ternary quadratic forms" by Friedlander and Iwaniec [4], in which they apply results from the afore-mentioned paper [3]. In [4], Friedlander and Iwaniec count small solutions (x_1, x_2, x_3) of the equation

$$x_1^2 + x_2^2 - x_3^2 = D.$$

Open problems

- Improve the exponent $11/18$.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.
- Extend the results to general ternary quadratic forms.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.
- Extend the results to general ternary quadratic forms.
- Treat the case $n > 3$ along similar lines.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.
- Extend the results to general ternary quadratic forms.
- Treat the case $n > 3$ along similar lines.
- For Pythagorean triples, investigate what happens in the transition range between two asymptotic formulas around the point $N = q^{1/2}$.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.
- Extend the results to general ternary quadratic forms.
- Treat the case $n > 3$ along similar lines.
- For Pythagorean triples, investigate what happens in the transition range between two asymptotic formulas around the point $N = q^{1/2}$.
- Consider inhomogeneous congruences.

Open problems

- Improve the exponent $11/18$.
- Merge our method with Heath-Brown's to treat general moduli.
- Extend the results to general ternary quadratic forms.
- Treat the case $n > 3$ along similar lines.
- For Pythagorean triples, investigate what happens in the transition range between two asymptotic formulas around the point $N = q^{1/2}$.
- Consider inhomogeneous congruences.
- Consider higher degree congruences.

References

- S. Baier, A. Haldar, *Small Pythagorean triples modulo prime powers*, preprint, arXiv:2201.05871.
- S. Baier, A. Haldar, *Asymptotic behavior of small solutions of quadratic congruences in three variables modulo prime powers*, preprint, arXiv:2202.06759.
- S. Baier; D. Mazumder, *Diophantine approximation with prime restriction in real quadratic number fields*, Math. Z. 299, No. 1-2, 699–750 (2021).
- T. Cochrane, *On representing the multiple of a number by a quadratic form*, Acta Arith. 63, No. 3, 211–222 (1993).

References

- T. Cochrane, Z. Zhiyong, *Exponential sums with rational function entries*, Acta Arith. 95, No. 1, 67–95 (2000).
- H. Davenport; H. Heilbronn, *On indefinite quadratic forms in five variables*, J. Lond. Math. Soc. 21, 185–193 (1946).
- W. Duke, J.B. Friedlander, H. Iwaniec, *Weyl sums for quadratic roots*, Int. Math. Res. Not. 2012, No. 11, 2493–2549 (2012).
- J. B. Friedlander, H. Iwaniec, *Small representations by indefinite ternary quadratic forms*, Borwein, Jonathan M. (ed.) et al., Number theory and related fields. In memory of Alf van der Poorten. Springer Proceedings in Mathematics & Statistics 43, 157-164 (2013).

References

- A.H. Hakami, *Small primitive zeros of quadratic forms mod p^m*, Ramanujan J. 38, No. 1, 189–198 (2015).
- D.R. Heath-Brown, *Small solutions of quadratic congruences*, Glasg. Math. J. 27, 87–93 (1985).
- D.R. Heath-Brown, *Small solutions of quadratic congruences. II*, Mathematika 38, No. 2, 264–284 (1991).
- D.R. Heath-Brown, *Small solutions of quadratic congruences, and character sums with binary quadratic forms*, Mathematika 62, No. 2, 551–571 (2016).
- W.G. Nowak, W. Recknagel, *The distribution of Pythagorean triples and a three-dimensional divisor problem*, Math. J. Okayama Univ. 31, 213–220 (1989).

References

A. Schinzel, H.P. Schlickewei, W.M. Schmidt, *Small solutions of quadratic congruence and small fractional parts of quadratic forms*, Acta Arith. 37, 241–248 (1980).

T. Laszlo, *Counting solutions of quadratic congruences in several variables revisited* , Journal of integer sequences, 17, 14.11.6 (2014).

J. Shurman, *Rational parametrization of conics*, online notes at http://people.reed.edu/~jerry/131/conics.pdf.

E.M. Stein, R. Shakarchi, *Fourier analysis. An Introduction*, Princeton Lectures in Analysis. 1. Princeton, NJ: Princeton University Press. xvi, 311 p. (2003).

Thank you for your kind attention!