Squares in Arithmetic Progressions

Brandon Boggess

March 24, 2020

Introduction

The first 10 perfect squares are

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100$$

Introduction

The first 10 perfect squares are

$$\mathbf{1}, 4, 9, 16, \mathbf{25}, 36, \mathbf{49}, 64, 81, 100$$

Introduction

- An *arithmetic progression* is a sequence

$$a, a + q, a + 2q, \ldots$$

- Question: How many of the numbers in an arithmetic progression can be squares?

Examples

- 1, 25, 49
  - $a = 1, q = 24$
- 289, 625, 961
  - $a = 289, q = 336$
- 529, 1369, 2209
  - $a = 529, q = 840$

Notation

- Fix $q, a > 0$
- $Q(N; q, a)$ is number of perfect squares $a + qn$ with $0 \leq n < N$
- $Q(N)$ is maximum over all a and all q

Rudin's Conjecture

Conjecture

$Q(N) = O(\sqrt{N})$

- This means that there is a constant C such that $Q(N) \leq C\sqrt{N}$, at least for N big enough
- This is a *uniform* bound – the constant does not depend on the particular arithmetic progression

Approach

Two step process

1. There can not be "long" arithmetic progressions of squares
2. Use this packing information to perform some combinatorics

Approach

First manifestation

1. There are no four squares in an arithmetic progression (Euler)
   - Counting rational points on curves
2. Large sets must contain long arithmetic progressions
   - Szemerédi's theorem

4 Squares in AP

- a^2, b^2, c^2, d^2 are in an AP if and only if

$$b^2 - a^2 = c^2 - b^2 = d^2 - c^2$$

- A little algebra gives

$$a^2 + c^2 = 2b^2, \quad b^2 + d^2 = 2c^2$$

- Upshot: $(a : b : c : d) \in \mathbf{P}^3(\mathbf{Q})$ lies on a projective curve

Aside on point counting

Let $C/\mathbf{Q}$ be a projective curve of genus g.

- $g = 0$: $C(\mathbf{Q})$ is infinite
- $g = 1$: $C(\mathbf{Q})$ is a finitely generated abelian group
- $g > 1$: $C(\mathbf{Q})$ is finite

4 Squares in AP

- Curve in $\mathbf{P}^3$ with equations

$$a^2 + c^2 = 2b^2, \quad b^2 + d^2 = 2c^2$$

- 8 silly points $(1 : \pm 1 : \pm 1 : \pm 1)$
- $g = 1$ (adjunction)
- Can be written in Weierstrass form

$$y^2 = x^3 - x^2 - 4x + 4$$

by projecting onto $\mathbf{P}^2$

4 Square in AP

- $y^2 = x^3 - x^2 - 4x + 4$
- Torsion subgroup is $\mathbf{Z}/8\mathbf{Z}$ (8 silly points)
- Rank is 0, so no 4 squares in arithmetic progression!

Szemerédi's Theorem

Theorem

Let $\delta > 0$. There exists N such that every subset of $\{1, \ldots, N\}$ of size δN has a four term arithmetic progression.

Szemerédi's Theorem

Theorem

Let $\delta > 0$. There exists N such that every subset of $\{1, \ldots, N\}$ of size δN has a four term arithmetic progression.

Apply to $\{n \leq N \mid qn + a \text{ is a square}\}$. Implies that $Q(N) = o(N)$

Proposition

$Q(N) = o(N)$

- Still a long way off of conjectured $O(N^{1/2})$
- Behrend: Szemerédi's argument cannot be used to get a smaller power

Bombieri-Granville-Pintz

Try to use simpler combinatorics and more complicated arithmetic geometry

Theorem

$Q(N) = O(N^{2/3}(\log N)^{c_2})$

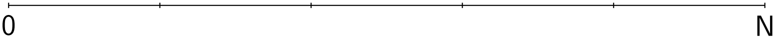
Outline

- Idea: “Most” boxes have a bounded number of points

Outline

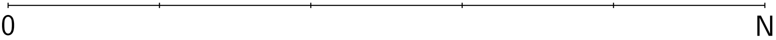
- Idea: "Most" boxes have a bounded number of points
- A box with five squares gives a point on a curve of genus 5

Outline



- Idea: “Most” boxes have a bounded number of points
- A box with five squares gives a point on a curve of genus 5
- By picking boxes of just the right size, get a good bound

Outline



- Idea: "Most" boxes have a bounded number of points
- A box with five squares gives a point on a curve of genus 5
- By picking boxes of just the right size, get a good bound
- WARNING: these points are not all on the same curve, and number of curves depends on the size of the boxes

Close Squares

- Let $1 \leq k_1 < \ldots < k_r$ integers
- If $b, b + k_1 d, \ldots, b + k_r d$ are all squares, (b, d) is a point on a curve $C_{\vec{k}}$ of genus
$$(r-3)2^{r-2} + 1$$
- $r = 3$ and $(k_i) = (1, 2, 3)$ is 4 squares in AP

Close Squares

- Let $1 \leq k_1 < \ldots < k_r$ integers
- If $b, b + k_1 d, \ldots, b + k_r d$ are all squares, (b, d) is a point on a curve $C_{\vec{k}}$ of genus
$$(r-3)2^{r-2} + 1$$
- $r = 3$ and $(k_i) = (1, 2, 3)$ is 4 squares in AP

We will consider points on many of these curves at once!

Recall

Let $C/\mathbf{Q}$ be a projective curve of genus g.

- $g = 0$: $C(\mathbf{Q})$ is infinite
- $g = 1$: $C(\mathbf{Q})$ is a finitely generated abelian group
- $g > 1$: $C(\mathbf{Q})$ is finite

Recall

Let $C/\mathbf{Q}$ be a projective curve of genus g.

- $g = 0$: $C(\mathbf{Q})$ is infinite
- $g = 1$: $C(\mathbf{Q})$ is a finitely generated abelian group
- $g > 1$: $C(\mathbf{Q})$ is finite

Smallest r for which curve has genus at least 2 is $r = 4$ (genus 5)

- All genus 5 curves have finitely many rational points
- In order to get an improved upper bound, need something even stronger

- All genus 5 curves have finitely many rational points
- In order to get an improved upper bound, need something even stronger

Theorem (Faltings,Vojta,Bombieri)

Let $C/\mathbf{Q}$ be a curve of genus at least 2. There is an explicit upper bound for $C(\mathbf{Q})$ in terms of the coefficients of the equations defining C and the rank of the Jacobian of C.

Jacobians of Curves

- The Jacobian of a curve C is an abelian variety containing C
- The dimension of J is the genus of G
- $J(\mathbf{Q})$ is a finitely generated abelian group

Jacobians of Curves

- The Jacobian of a curve C is an abelian variety containing C
- The dimension of J is the genus of G
- $J(\mathbf{Q})$ is a finitely generated abelian group
- E.g. if C is an elliptic curve, $J \simeq C$

Jacobians in BGP

- The Jacobians of $C_{\vec{k}}$ are products of elliptic curves

Jacobians in BGP

- The Jacobians of $C_{\vec{k}}$ are products of elliptic curves
- In fact, these elliptic curves have full 2 torsion!
  - $y^2 = (x - e_1)(x - e_2)(x - e_3)$

Jacobians in BGP

- The Jacobians of $C_{\vec{k}}$ are products of elliptic curves
- In fact, these elliptic curves have full 2 torsion!
  - $y^2 = (x - e_1)(x - e_2)(x - e_3)$
- 2-descent lets you bound the ranks of the elliptic curves (cf Silverman)

This is used to prove

Corollary

Fix $\varepsilon > 0$. If $1 \leq k_1 < \cdots < k_4 \leq N$, then there are at most CN^{ε} squares of the form $b, b + k_1 d, \ldots, b + k_4 d$ with d larger than some explicit constant. Here C depends only on ε

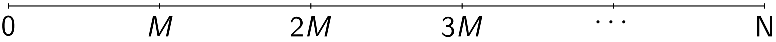
This is an explicit bound on the number of boxes which can contain 5 squares

Corollary

Fix $\varepsilon > 0$. If $1 \leq k_1 < \cdots < k_4 \leq N$, then there are at most CN^{ε} squares of the form $b, b + k_1 d, \ldots, b + k_4 d$ with d larger than some explicit constant. Here C depends only on ε

Corollary

Fix $\varepsilon > 0$. If $1 \leq k_1 < \cdots < k_4 \leq N$, then there are at most CN^{ε} squares of the form $b, b + k_1 d, \ldots, b + k_4 d$ with d larger than some explicit constant. Here C depends only on ε



- If one box has 5 squares, get $b, b + k_1 d, \ldots, b + k_4 d$ all squares with $1 \leq k_1 < \cdots < k_4 \leq M$
- By the theorem, at most $M^{4+\varepsilon}$ of these

Corollary

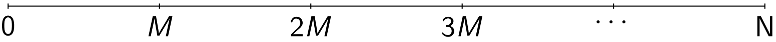
Fix $\varepsilon > 0$. If $1 \leq k_1 < \cdots < k_4 \leq N$, then there are at most CN^{ε} squares of the form $b, b + k_1 d, \ldots, b + k_4 d$ with d larger than some explicit constant. Here C depends only on ε

$$0 \quad M \quad 2M \quad 3M \quad \cdots \quad N$$

- If one box has 5 squares, get $b, b + k_1 d, \ldots, b + k_4 d$ all squares with $1 \leq k_1 < \cdots < k_4 \leq M$
- By the theorem, at most $M^{4+\varepsilon}$ of these
- Boxes with few squares contribute at most N/M

Corollary

Fix $\varepsilon > 0$. If $1 \leq k_1 < \cdots < k_4 \leq N$, then there are at most CN^{ε} squares of the form $b, b + k_1 d, \ldots, b + k_4 d$ with d larger than some explicit constant. Here C depends only on ε



- If one box has 5 squares, get $b, b + k_1 d, \ldots, b + k_4 d$ all squares with $1 \leq k_1 < \cdots < k_4 \leq M$
- By the theorem, at most $M^{4+\varepsilon}$ of these
- Boxes with few squares contribute at most N/M
- In total: $N/M + M^{4+\varepsilon}$

- This only gets you $Q(N) = O(N^{4/5+\varepsilon})$
- A sieve technique brings the exponent down to $2/3 + \varepsilon$

- This only gets you $Q(N) = O(N^{4/5+\varepsilon})$
- A sieve technique brings the exponent down to $2/3 + \varepsilon$
- Same techniques work for kth powers in APs, except elliptic curves don't have 2-torsion!
- Descent must be done over cyclotomic fields