Diophantine Tuples over $\mathbb{Z}_p$

Simon Rubinstein-Salzedo
simon@eulercircle.com

(Joint work with Nitya Mani)

Euler Circle

18 December, 2018

Diophantine Tuples

Definition

A *Diophantine m-tuple* is a tuple $(a_1, a_2, \ldots, a_m)$ of positive integers such that whenever $1 \leq i, j \leq m$, $i \neq j$, $a_i a_j + 1$ is a perfect square.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.
- Euler: Extended Fermat's quadruple to a quintuple $\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.
- Euler: Extended Fermat's quadruple to a quintuple $\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$.
- Baker and Davenport: Used then-novel method of linear forms in logarithms to prove that the only extension of $(1, 3, 8)$ to a quadruple in the positive integers is Fermat's example.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.
- Euler: Extended Fermat's quadruple to a quintuple $\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$.
- Baker and Davenport: Used then-novel method of linear forms in logarithms to prove that the only extension of $(1, 3, 8)$ to a quadruple in the positive integers is Fermat's example.
- Gibbs: Found a rational sextuple $\left(\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right)$.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.
- Euler: Extended Fermat's quadruple to a quintuple $\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$.
- Baker and Davenport: Used then-novel method of linear forms in logarithms to prove that the only extension of $(1, 3, 8)$ to a quadruple in the positive integers is Fermat's example.
- Gibbs: Found a rational sextuple $\left(\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right)$.
- Dujella: No sextuples in the positive integers, and only finitely many quintuples.

History

- Diophantus: Found the quadruple $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$.
- Fermat: Found the quadruple $(1, 3, 8, 120)$.
- Euler: Showed that any triple can be extended to a quadruple.
- Euler: Extended Fermat's quadruple to a quintuple $\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$.
- Baker and Davenport: Used then-novel method of linear forms in logarithms to prove that the only extension of $(1, 3, 8)$ to a quadruple in the positive integers is Fermat's example.
- Gibbs: Found a rational sextuple $\left(\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right)$.
- Dujella: No sextuples in the positive integers, and only finitely many quintuples.
- He, Togbé, Ziegler: No Diophantine quintuples in positive integers.

The $D(r)$ property

Definition

A $D(r)$ *m-tuple* is a tuple $(a_1, a_2, \ldots, a_m)$ such that whenever $1 \leq i, j \leq m$, $i \neq j$, $a_i a_j + r$ is a perfect square.

The $D(r)$ property

Definition

A $D(r)$ *m-tuple* is a tuple $(a_1, a_2, \ldots, a_m)$ such that whenever $1 \leq i, j \leq m$, $i \neq j$, $a_i a_j + r$ is a perfect square.

Example

Diophantus's example $\left(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right)$ can be converted into a $D(256)$ quadruple by clearing denominators: $(1, 33, 68, 105)$ is a $D(256)$ quadruple.

Notation

Let R be a commutative ring, equipped with a probability measure μ.

- $\square(R)$ is the set of squares in R, i.e. $\{a \in R : \exists b \in R \text{ with } b^2 = a\}$.
- $\text{Dioph}_m^r(R) = \{(a_1, \ldots, a_m) \in R : a_i a_j + r \in \square(R) \text{ for } 1 \leq i, j \leq m, i \neq j\}$.
- $\text{dioph}_m^r(R) = \mu(\text{Dioph}_m^r(R))$.

Goal

$R = \mathbb{Z}_p$, the ring of p-adic numbers, μ the normalized Haar measure on $\mathbb{Z}_p$. Compute or estimate $\mathrm{dioph}_m^r(R)$.

Squares in $\mathbb{Z}_p$

Any nonzero element in $\mathbb{Z}_p$ can be written uniquely in the form ap^n, where $p \nmid a$ and n is a nonnegative integer.

Proposition

$a2^n$ is a square in $\mathbb{Z}_2$ if and only if $a \equiv 1 \pmod 8$ and n is even.

Proposition

ap^n is a square in $\mathbb{Z}_p$ for p odd if and only if $\left(\frac{a}{p}\right) = 1$ and n is even.

Heuristic

We expect that, for fixed m and r, and $p \to \infty$, $\mathrm{dioph}_m^r(\mathbb{Z}_p) \approx \frac{1}{2^{\binom{m}{2}}}$.

Heuristic

We expect that, for fixed m and r, and $p \to \infty$, $\mathrm{dioph}_m^r(\mathbb{Z}_p) \approx \frac{1}{2^{\binom{m}{2}}}$.

Roughly $\frac{1}{2}$ chance that each $a_i a_j + r \in \square(\mathbb{Z}_p)$, and they're fairly independent.

Heuristic

We expect that, for fixed m and r, and $p \to \infty$, $\mathrm{dioph}_m^r(\mathbb{Z}_p) \approx \frac{1}{2^{\binom{m}{2}}}$.

Roughly $\frac{1}{2}$ chance that each $a_i a_j + r \in \square(\mathbb{Z}_p)$, and they're fairly independent.

Possible correction: that doesn't work when some $a_i a_j + r \equiv 0 \pmod{p}$, so maybe $\mathrm{dioph}_m^r(\mathbb{Z}_p) = \frac{1}{2^{\binom{m}{2}}} + O\left(\frac{1}{p}\right)$.

Heuristic

We expect that, for fixed m and r, and $p \to \infty$, $\mathrm{dioph}_m^r(\mathbb{Z}_p) \approx \frac{1}{2^{\binom{m}{2}}}$.

Roughly $\frac{1}{2}$ chance that each $a_i a_j + r \in \square(\mathbb{Z}_p)$, and they're fairly independent.

Possible correction: that doesn't work when some $a_i a_j + r \equiv 0 \pmod{p}$, so maybe $\mathrm{dioph}_m^r(\mathbb{Z}_p) = \frac{1}{2^{\binom{m}{2}}} + O\left(\frac{1}{p}\right)$.

True for small m only, since there's a second correction coming from failure of independence. For $m \geq 4$, we only get $\mathrm{dioph}_m^r(\mathbb{Z}_p) = \frac{1}{2^{\binom{m}{2}}} + O\left(\frac{1}{\sqrt{p}}\right)$.

$\mathrm{dioph}_2^1(\mathbb{Z}_2)$

Proposition

$\mathrm{dioph}_2^1(\mathbb{Z}_2) = \frac{1}{3}$.

$\mathrm{dioph}_2^1(\mathbb{Z}_2)$

Proposition

$\mathrm{dioph}_2^1(\mathbb{Z}_2) = \frac{1}{3}$.

Proof.

Let $A_{2k} = \{(a,b) \in \mathrm{Dioph}_2^1(\mathbb{Z}_2) : v_2(ab+1) = 2k\}$. We can calculate that $\mu(A_0) = \frac{5}{16}$ and $\mu(A_{2k}) = \frac{1}{2^{2k+4}}$ for $k \geq 1$. Thus

$$\mathrm{dioph}_2^1(\mathbb{Z}_2) = \frac{5}{16} + \sum_{k=1}^{\infty} \frac{1}{2^{2k+4}} = \frac{1}{3}.$$

$\mathrm{dioph}_2^r(\mathbb{Z}_p)$

When p is odd, we can always compute $\mathrm{dioph}_2^r(\mathbb{Z}_p)$ exactly.

Theorem

Let p be an odd prime and let $\alpha = v_p(r)$ with $r = p^\alpha s$. Then, we have the following:

$$\mathrm{dioph}_2^r(\mathbb{Z}_p) = \begin{cases} \frac{1}{2} + \frac{1}{p(p+1)} & \left(\frac{r}{p}\right) = 1 \\ \frac{1}{2} - \frac{1}{p+1} & \left(\frac{r}{p}\right) = -1 \\ \frac{1}{2} - \frac{p-1}{2(p+1)^2} - \frac{(\alpha+2)}{2(p+1)^2 p^{\alpha-1}} - \frac{1}{2(p+1)^2 p^\alpha} + \frac{(\alpha-1)}{2(p+1)^2 p^{\alpha+1}} & \alpha \equiv 1 \pmod 2 \\ \frac{1}{2} + \frac{(\alpha+1)(p-1)^2}{2p^{\alpha+2}} - \frac{2p-1}{2(p+1)^2} + \frac{1}{2(p+1)^2 p} - \frac{(\alpha+1)}{2(p+1)^2 p^{\alpha-2}} & \\ \quad + \frac{(\alpha-1)}{2(p+1)^2 p^\alpha} - \frac{1}{2(p+1)^2 p^{\alpha+1}} - \frac{1}{2(p+1)^2 p^{\alpha+2}} & \alpha > 0 \text{ even}, \left(\frac{s}{p}\right) = -1 \\ \frac{1}{2} + \frac{\alpha(p-1)^2+p^2+1}{2p^{\alpha+2}} - \frac{2p-1}{2(p+1)^2} + \frac{1}{2(p+1)^2 p} - \frac{(\alpha+1)}{2(p+1)^2 p^{\alpha-2}} & \\ \quad + \frac{(\alpha-1)}{2(p+1)^2 p^\alpha} - \frac{1}{2(p+1)^2 p^{\alpha+1}} - \frac{1}{2(p+1)^2 p^{\alpha+2}} & \alpha > 0 \text{ even}, \left(\frac{s}{p}\right) = 1. \end{cases}$$

In particular, we have that the measure of the Diophantine pairs over $\mathbb{Z}_p$ is given by

$$\mathrm{dioph}_2^1(\mathbb{Z}_p) = \frac{1}{2} + \frac{1}{p(p+1)}.$$

$\mathrm{dioph}_m^r(\mathbb{Z}_3)$

When $r \equiv 1 \pmod 3$, we can calculate $\mathrm{dioph}_m^r(\mathbb{Z}_3)$ exactly for all m.

Theorem

For any $r \in \mathbb{Z}_3$ with $\left(\frac{r}{3}\right) = 1$ and $m \geq 1$, we have

$$\mathrm{dioph}_m^r(\mathbb{Z}_3) = \frac{m^2 + 71m + 36}{36 \cdot 3^m}.$$

$\mathrm{dioph}_m^r(\mathbb{Z}_3)$

When $r \equiv 1 \pmod 3$, we can calculate $\mathrm{dioph}_m^r(\mathbb{Z}_3)$ exactly for all m.

Theorem

For any $r \in \mathbb{Z}_3$ with $\left(\frac{r}{3}\right) = 1$ and $m \geq 1$, we have

$$\mathrm{dioph}_m^r(\mathbb{Z}_3) = \frac{m^2 + 71m + 36}{36 \cdot 3^m}.$$

Idea: at most one a_i can be $1 \pmod 3$, and at most one a_j can be $-1 \pmod 3$. Then $a_i a_j + r \in \square(\mathbb{Z}_3)$ whenever $a_i a_j \equiv 0 \pmod 3$, so we only have to worry about the (at most) one pair where $a_i a_j \not\equiv 0 \pmod 3$.

$\mathrm{dioph}_3^r(\mathbb{Z}_p)$

Let p be an odd prime. We can't calculate $\mathrm{dioph}_3^r(\mathbb{Z}_p)$ exactly, but we can calculate $\mathrm{dioph}_3^r(\mathbb{F}_p)$ exactly.

Theorem

If $p \nmid r$, then

$$\mathrm{dioph}_3^r(\mathbb{F}_p) = \frac{1}{8} + \frac{1}{p} \cdot \left(\frac{5}{8} + \frac{3}{8} \left(\frac{r}{p} \right) \right) + \frac{1}{p^2} \left(\frac{25}{8} + \left(\frac{r}{p} \right) \right) - \frac{1}{p^3} \left(\frac{15}{8} + \frac{25}{8} \left(\frac{r}{p} \right) - \frac{7}{2} \left(\frac{-r}{p} \right) \right).$$

A Useful Lemma

Lemma

Let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_p[x]$ and $a_2 \neq 0$. Let $\Delta = a_1^2 - 4a_0a_2$ be the discriminant of f. Then,

$$\sum_{c \in \mathbb{F}_p} \left(\frac{f(c)}{p} \right) = \begin{cases} -\left(\frac{a_2}{p}\right) & \Delta \neq 0 \\ (p-1)\left(\frac{a_2}{p}\right) & \Delta = 0. \end{cases}$$

Idea of Proof

Worry about the cases where $abc(ab+r)(ac+r)(bc+r) \equiv 0 \pmod{p}$ separately. Otherwise, we have

$$
\begin{aligned}
&\#\left\{(a,b,c) \in \mathrm{Diophant}_3^r(\mathbb{F}_p) : (ab+r)(bc+r)(ac+r)abc \not\equiv 0 \pmod{p}\right\} \\
&= \frac{1}{8}\sum_{c=1}^{p-1}\sum_{b=1}^{p-1}\sum_{a=1}^{p-1} \mathbb{1}_{\{(ab+r)(bc+r)(ac+r)\neq 0\}} \left(1+\left(\frac{ab+r}{p}\right)\right)\left(1+\left(\frac{bc+r}{p}\right)\right)\left(1+\left(\frac{ac+r}{p}\right)\right) \\
&= \frac{1}{8}\sum_{\gamma=1}^{p-1}\sum_{\beta=1}^{p-1}\sum_{\alpha=1}^{p-1} \mathbb{1}_{\{(\alpha+r)(\beta+r)(\alpha\beta\gamma^2+r)\neq 0\}} \left(1+\left(\frac{\alpha+r}{p}\right)\right)\left(1+\left(\frac{\beta+r}{p}\right)\right)\left(1+\left(\frac{\alpha\beta\gamma^2+r}{p}\right)\right) \\
&= \frac{1}{8}\sum_{\gamma=1}^{p-1}\sum_{\beta=1+r}^{p-1+r}\sum_{\alpha=1+r}^{p-1+r} \mathbb{1}_{\{\alpha\beta((\alpha-r)(\beta-r)\gamma^2+r)\neq 0\}} \left(1+\left(\frac{\alpha}{p}\right)\right)\left(1+\left(\frac{\beta}{p}\right)\right)\left(1+\left(\frac{(\alpha-r)(\beta-r)\gamma^2+r}{p}\right)\right) \\
&= \frac{1}{8}\sum_{\beta=1+r}^{p-1+r}\sum_{\alpha=1+r}^{p-1+r} \mathbb{1}_{\{\alpha\beta\neq 0\}} \left(1+\left(\frac{\alpha}{p}\right)\right)\left(1+\left(\frac{\beta}{p}\right)\right)\sum_{\gamma=1}^{p-1} \mathbb{1}_{\{(\alpha-r)(\beta-r)\gamma^2+r\neq 0\}} \left(1+\left(\frac{(\alpha-r)(\beta-r)\gamma^2+r}{p}\right)\right).
\end{aligned}
$$

Back to $\mathrm{dioph}_3^r(\mathbb{Z}_p)$

To estimate $\mathrm{dioph}_3^r(\mathbb{Z}_p)$ from $\mathrm{dioph}_3^r(\mathbb{F}_p)$, note that if $abc(ab+r)(ac+r)(bc+r) \not\equiv 0 \pmod{p}$, then $(a,b,c) \in \mathrm{Dioph}_3^r(\mathbb{Z}_p)$ if and only if its reduction lies in $\mathrm{Dioph}_3^r(\mathbb{F}_p)$. Thus we have

$$|\mathrm{dioph}_3^r(\mathbb{F}_p) - \mathrm{dioph}_3^r(\mathbb{Z}_p)| \leq \frac{6}{p}.$$

So

$$\mathrm{dioph}_3^r(\mathbb{Z}_p) = \frac{1}{8} + O\left(\frac{1}{p}\right).$$

$m \geq 4$

We can no longer exactly compute $\mathrm{dioph}_m^r(\mathbb{F}_p)$, because there is no exact form for computing the character sums $\sum_{c \in \mathbb{F}_p} \left(\frac{f(c)}{p}\right)$ when $\deg f \geq 3$. Instead, we need to count points on a hyperelliptic curve.

Theorem (Hasse-Weil)

Let C be a smooth curve of genus g over a finite field $\mathbb{F}_q$. Then

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

Or, the character sum version:

Theorem

Let $f(x) \in \mathbb{F}_q[x]$ be a monic squarefree polynomial of degree d. Then

$$\left| \sum_{c \in \mathbb{F}_q} \left(\frac{f(c)}{p}\right) \right| \leq (d-1)\sqrt{q}.$$

$m \geq 4$

Using similar methods to the $m = 3$ case and the character sum bound, we can prove the following:

Theorem

For fixed $m \geq 3$ and $r \in \mathbb{Z}$, as $p \to \infty$ we have

$$\mathrm{diophr}_m^r(\mathbb{F}_p) = \frac{1}{2^{\binom{m}{2}}} + O\left(\frac{1}{\sqrt{p}}\right).$$

Since $\left|\mathrm{diophr}_m^r(\mathbb{F}_p) - \mathrm{diophr}_m^r(\mathbb{Z}_p)\right| \leq \frac{m+\binom{m}{2}}{p-1}$, we also have

$$\mathrm{diophr}_m^r(\mathbb{Z}_p) = \frac{1}{2^{\binom{m}{2}}} + O\left(\frac{1}{\sqrt{p}}\right).$$

Thank you

Thank you for your attention!