Squarefree values of trinomial discriminants

Greg Martin
University of British Columbia

joint work with David Boyd and Mark Thom

AMS Special Session on Analytic Number Theory
Joint Mathematics Meetings of the AMS and MAA
Baltimore, MD
January 17, 2014

slides can be found on my web page
www.math.ubc.ca/∼gerg/index.shtml?slides

Outline

1. Discriminants of trinomials
2. Primes whose squares can divide trinomial discriminants
3. Conjecture on the proportion of squarefree values
4. (if time) A new family of ABC triples

A freaky divisibility

LIke nothing I've seen before

For any nonnegative integer k,

$$(12k^2 + 6k + 1)^2 \quad \text{divides} \quad (6k + 2)^{6k+2} - (6k + 1)^{6k+1}.$$

If you're bored during the talk, you can prove it by hand.

Hint:

With $M = 12k^2 + 6k + 1$, start by verifying that

$$-(6k + 2)^3 \equiv 1 - (18k + 9) \cdot M \pmod{M^2}$$

$$(6k + 1)^3 \equiv 1 + 18k \cdot M \pmod{M^2}.$$

A freaky divisibility

LIke nothing I've seen before

For any nonnegative integer k,

$$(12k^2+6k+1)^2 \quad \text{divides} \quad (6k+2)^{6k+2}-(6k+1)^{6k+1}.$$

If you're bored during the talk, you can prove it by hand.

Hint:

With $M = 12k^2+6k+1$, start by verifying that

$$-(6k+2)^3 \equiv 1-(18k+9)\cdot M \pmod{M^2}$$

$$(6k+1)^3 \equiv 1+18k\cdot M \pmod{M^2}.$$

Discriminants of trinomials (background)

We started caring about the expression $n^n - (n-1)^{n-1}$ because it's the discriminant of the trinomial $x^n - x + 1$.

Motivation

Let θ be a root of $x^n - x + 1$. We were interested in whether $n^n - (n-1)^{n-1}$ was squarefree because if it is, then the ring of integers in $\mathbb{Q}(\theta)$ has a power basis—it's simply $\mathbb{Z}[\theta]$.

Of course, we should only consider this when $x^n - x + 1$ is irreducible. . . .

Discriminants of trinomials (background)

We started caring about the expression $n^n - (n-1)^{n-1}$ because it's the discriminant of the trinomial $x^n - x + 1$.

Motivation

Let θ be a root of $x^n - x + 1$. We were interested in whether $n^n - (n-1)^{n-1}$ was squarefree because if it is, then the ring of integers in $\mathbb{Q}(\theta)$ has a power basis—it's simply $\mathbb{Z}[\theta]$.

Of course, we should only consider this when $x^n - x + 1$ is irreducible. . . .

Discriminants of trinomials (background)

We started caring about the expression $n^n - (n-1)^{n-1}$ because it's the discriminant of the trinomial $x^n - x + 1$.

Motivation

Let θ be a root of $x^n - x + 1$. We were interested in whether $n^n - (n-1)^{n-1}$ was squarefree because if it is, then the ring of integers in $\mathbb{Q}(\theta)$ has a power basis—it's simply $\mathbb{Z}[\theta]$.

Of course, we should only consider this when $x^n - x + 1$ is irreducible. . . .

A resultant divisibility

When $n = 6k+2$, the polynomial is reducible:

$$x^{6k+2} - x + 1 = (x^2 - x + 1)g(x)$$

for some polynomial $g(x)$.

A "product rule" for discriminants

$$\operatorname{Disc}(fg) = \operatorname{Disc}(f)\operatorname{Disc}(g)\operatorname{Res}(f,g)^2$$

In our situation,

$$\operatorname{Res}(x^2 - x + 1, g(x))^2 \mid \operatorname{Disc}(x^{6k+2} - x + 1)$$

$$(12k^2 + 6k + 1)^2 \mid \left((6k+2)^{6k+2} - (6k+1)^{6k+1}\right)$$

A resultant divisibility

When $n = 6k+2$, the polynomial is reducible:

$$x^{6k+2} - x + 1 = (x^2 - x + 1)g(x)$$

for some polynomial $g(x)$.

A "product rule" for discriminants

$$\mathrm{Disc}(fg) = \mathrm{Disc}(f)\,\mathrm{Disc}(g)\,\mathrm{Res}(f,g)^2$$

In our situation,

$$\begin{aligned}\mathrm{Res}(x^2 - x + 1, g(x))^2 &\mid \mathrm{Disc}(x^{6k+2} - x + 1)\\ (12k^2 + 6k + 1)^2 &\mid \big((6k+2)^{6k+2} - (6k+1)^{6k+1}\big)\end{aligned}$$

A resultant divisibility

When $n = 6k + 2$, the polynomial is reducible:

$$x^{6k+2} - x + 1 = (x^2 - x + 1)g(x)$$

for some polynomial $g(x)$.

A “product rule” for discriminants

$$\mathrm{Disc}(fg) = \mathrm{Disc}(f)\,\mathrm{Disc}(g)\,\mathrm{Res}(f, g)^2$$

In our situation,

$$\begin{aligned} \mathrm{Res}(x^2 - x + 1, g(x))^2 &\mid \mathrm{Disc}(x^{6k+2} - x + 1) \\ (12k^2 + 6k + 1)^2 &\mid \big((6k + 2)^{6k+2} - (6k + 1)^{6k+1}\big) \end{aligned}$$

A resultant divisibility

When $n = 6k + 2$, the polynomial is reducible:

$$x^{6k+2} - x + 1 = (x^2 - x + 1)g(x)$$

for some polynomial $g(x)$.

A "product rule" for discriminants

$$\mathrm{Disc}(fg) = \mathrm{Disc}(f)\,\mathrm{Disc}(g)\,\mathrm{Res}(f, g)^2$$

In our situation,

$$\begin{aligned} \mathrm{Res}(x^2 - x + 1, g(x))^2 &\mid \mathrm{Disc}(x^{6k+2} - x + 1) \\ (12k^2 + 6k + 1)^2 &\mid \big((6k + 2)^{6k+2} - (6k + 1)^{6k+1}\big) \end{aligned}$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n(n-1)^{n-1}$.

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree* for $n \le 256$. * as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \big((2p-1)^{2p-1} + (2p-2)^{2p-2}\big).$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n(n-1)^{n-1}$.

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree* for $n \le 256$.

* as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \big((2p-1)^{2p-1} + (2p-2)^{2p-2}\big).$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n(n-1)^{n-1}$.

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree* for $n \le 256$.

* as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \left((2p-1)^{2p-1} + (2p-2)^{2p-2}\right).$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n(n-1)^{n-1}$.

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree* for $n \le 256$.

* as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \big((2p-1)^{2p-1} + (2p-2)^{2p-2}\big).$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n (n-1)^{n-1}$.

$n^n + (-1)^n (n-1)^{n-1}$ is squarefree* for $n \le 256$. * as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \big((2p-1)^{2p-1} + (2p-2)^{2p-2}\big).$$

Non-squarefree values

Change the polynomial

The polynomial $x^n - x - 1$ is always irreducible, and its discriminant is $n^n + (-1)^n(n-1)^{n-1}$.

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree* for $n \le 256$.

* as far as we can tell!

Nothing lasts forever

- $59^2 \mid (257^{257} - 256^{256})$
- other numerical examples
- if $2^p \equiv 2 \pmod{p^2}$ (so that p is a Wieferich prime),

$$p^2 \mid \big((2p-1)^{2p-1} + (2p-2)^{2p-2}\big).$$

Which primes can divide trinomial discriminants?

The theory is tidier if we study the more general expression

$$n^n \pm m^m(n-m)^{n-m},$$

which arises in the discriminants of trinomials $x^n \pm x^m \pm 1$.

Definition

$\mathcal{P}_+ = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n + m^m(n-m)^{n-m})\}$

$\mathcal{P}_- = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n - m^m(n-m)^{n-m})\}$

- (in both cases, prohibit trivialities such as $p \mid m$, $p \mid n$)

From the examples on the last slide:

- $59 \in \mathcal{P}_-$ $(n = 257, m = 1)$
- Wieferich primes are in $\mathcal{P}_+$ $(n = 2p-1, m = 1)$

Which primes can divide trinomial discriminants?

The theory is tidier if we study the more general expression

$$n^n \pm m^m (n-m)^{n-m},$$

which arises in the discriminants of trinomials $x^n \pm x^m \pm 1$.

Definition

$\mathcal{P}_+ = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid \big(n^n + m^m (n-m)^{n-m}\big)\}$

$\mathcal{P}_- = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid \big(n^n - m^m (n-m)^{n-m}\big)\}$

- (in both cases, prohibit trivialities such as $p \mid m$, $p \mid n$)

From the examples on the last slide:

- $59 \in \mathcal{P}_-$ $(n = 257, m = 1)$
- Wieferich primes are in $\mathcal{P}_+$ $(n = 2p-1, m = 1)$

Which primes can divide trinomial discriminants?

The theory is tidier if we study the more general expression

$$n^n \pm m^m (n-m)^{n-m},$$

which arises in the discriminants of trinomials $x^n \pm x^m \pm 1$.

Definition

$\mathcal{P}_+ = \{p \colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n + m^m(n-m)^{n-m})\}$

$\mathcal{P}_- = \{p \colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n - m^m(n-m)^{n-m})\}$

- (in both cases, prohibit trivialities such as $p \mid m$, $p \mid n$)

From the examples on the last slide:

- $59 \in \mathcal{P}_-$ $(n = 257, m = 1)$
- Wieferich primes are in $\mathcal{P}_+$ $(n = 2p-1, m = 1)$

Which primes can divide trinomial discriminants?

The theory is tidier if we study the more general expression

$$n^n \pm m^m(n-m)^{n-m},$$

which arises in the discriminants of trinomials $x^n \pm x^m \pm 1$.

Definition

$\mathcal{P}_+ = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n + m^m(n-m)^{n-m})\}$

$\mathcal{P}_- = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid (n^n - m^m(n-m)^{n-m})\}$

- (in both cases, prohibit trivialities such as $p \mid m$, $p \mid n$)

From the examples on the last slide:

- $59 \in \mathcal{P}_-$ $(n = 257, m = 1)$
- Wieferich primes are in $\mathcal{P}_+$ $(n = 2p-1, m = 1)$

Which primes can divide trinomial discriminants?

The theory is tidier if we study the more general expression

$$n^n \pm m^m (n-m)^{n-m},$$

which arises in the discriminants of trinomials $x^n \pm x^m \pm 1$.

Definition

$\mathcal{P}_+ = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid \big(n^n + m^m(n-m)^{n-m}\big)\}$

$\mathcal{P}_- = \{p\colon \text{there exist } m, n \text{ such that } p^2 \mid \big(n^n - m^m(n-m)^{n-m}\big)\}$

- (in both cases, prohibit trivialities such as $p \mid m$, $p \mid n$)

From the examples on the last slide:

- $59 \in \mathcal{P}_-$ $(n = 257, m = 1)$
- Wieferich primes are in $\mathcal{P}_+$ $(n = 2p-1, m = 1)$

Another set of primes

Definition

$\mathcal{P}_{cons}$ is the set of primes p such that there exist two consecutive pth powers modulo p^2.

- (prohibit the trivialities $(-1)^p, 0^p, 1^p$)

Example

- $59 \in \mathcal{P}_{cons}$, since $4^{59} - 3^{59} \equiv 299 - 298 = 1 \pmod{59^2}$
- Wieferich primes are in $\mathcal{P}_{cons}$: $2^p - 1^p \equiv 2 - 1 = 1 \pmod{p^2}$

Remark

If $y^p - x^p \equiv 1 \pmod{p^2}$, then $(y-x)^p \equiv y^p - x^p \equiv 1 \pmod{p}$ and hence $y - x \equiv 1 \pmod{p}$. So the only pth powers that can possibly be consecutive are pairs $x^p, (x+1)^p$.

Another set of primes

Definition

$\mathcal{P}_{cons}$ is the set of primes p such that there exist two consecutive pth powers modulo p^2.

- (prohibit the trivialities $(-1)^p, 0^p, 1^p$)

Example

- $59 \in \mathcal{P}_{cons}$, since $4^{59} - 3^{59} \equiv 299 - 298 = 1 \pmod{59^2}$
- Wieferich primes are in $\mathcal{P}_{cons}$: $2^p - 1^p \equiv 2 - 1 = 1 \pmod{p^2}$

Remark

If $y^p - x^p \equiv 1 \pmod{p^2}$, then $(y-x)^p \equiv y^p - x^p \equiv 1 \pmod{p}$ and hence $y - x \equiv 1 \pmod{p}$. So the only pth powers that can possibly be consecutive are pairs $x^p, (x+1)^p$.

Another set of primes

Definition

$\mathcal{P}_{cons}$ is the set of primes p such that there exist two consecutive pth powers modulo p^2.

- (prohibit the trivialities $(-1)^p, 0^p, 1^p$)

Example

- $59 \in \mathcal{P}_{cons}$, since $4^{59} - 3^{59} \equiv 299 - 298 = 1 \pmod{59^2}$
- Wieferich primes are in $\mathcal{P}_{cons}$: $2^p - 1^p \equiv 2 - 1 = 1 \pmod{p^2}$

Remark

If $y^p - x^p \equiv 1 \pmod{p^2}$, then $(y-x)^p \equiv y^p - x^p \equiv 1 \pmod{p}$ and hence $y - x \equiv 1 \pmod{p}$. So the only pth powers that can possibly be consecutive are pairs $x^p, (x+1)^p$.

Another set of primes

Definition

$\mathcal{P}_{cons}$ is the set of primes p such that there exist two consecutive pth powers modulo p^2.

- (prohibit the trivialities $(-1)^p, 0^p, 1^p$)

Example

- $59 \in \mathcal{P}_{cons}$, since $4^{59} - 3^{59} \equiv 299 - 298 = 1 \pmod{59^2}$
- Wieferich primes are in $\mathcal{P}_{cons}$: $2^p - 1^p \equiv 2 - 1 = 1 \pmod{p^2}$

Remark

If $y^p - x^p \equiv 1 \pmod{p^2}$, then $(y-x)^p \equiv y^p - x^p \equiv 1 \pmod{p}$ and hence $y - x \equiv 1 \pmod{p}$. So the only pth powers that can possibly be consecutive are pairs $x^p, (x+1)^p$.

Don't I know you. . . ?

$\mathcal{P}_\pm = \{p\colon$ there exist m, n such that $p^2 \mid \big(n^n \pm m^m(n-m)^{n-m}\big)\}$
$\mathcal{P}_{cons} = \{p\colon$ there exist two consecutive pth powers modulo $p^2\}$

Theorem (Boyd, M., Thom, 2014)

$$\mathcal{P}_+ = \mathcal{P}_{cons} = \mathcal{P}_-$$

Remark

When $p \equiv 1 \pmod 3$, primitive 3rd and 6th roots of unity modulo p^2 are always consecutive. If we prohibit those from counting towards $\mathcal{P}_{cons}$, and we also prohibit "resultant divisibilities" from counting towards $\mathcal{P}_+$ and $\mathcal{P}_-$, then the theorem also holds for the more restrictive sets of primes.

Don't I know you. . . ?

$\mathcal{P}_\pm = \big\{p\colon \text{there exist } m,n \text{ such that } p^2 \mid \big(n^n \pm m^m(n-m)^{n-m}\big)\big\}$

$\mathcal{P}_{cons} = \{p\colon \text{there exist two consecutive } p\text{th powers modulo } p^2\}$

Theorem (Boyd, M., Thom, 2014)

$$\mathcal{P}_+ = \mathcal{P}_{cons} = \mathcal{P}_-$$

Remark

When $p \equiv 1 \pmod 3$, primitive 3rd and 6th roots of unity modulo p^2 are always consecutive. If we prohibit those from counting towards $\mathcal{P}_{cons}$, and we also prohibit "resultant divisibilities" from counting towards $\mathcal{P}_+$ and $\mathcal{P}_-$, then the theorem also holds for the more restrictive sets of primes.

Don't I know you. . . ?

$\mathcal{P}_\pm = \big\{p\colon \text{there exist } m, n \text{ such that } p^2 \mid \big(n^n \pm m^m(n-m)^{n-m}\big)\big\}$
$\mathcal{P}_{cons} = \{p\colon \text{there exist two consecutive } p\text{th powers modulo } p^2\}$

Theorem (Boyd, M., Thom, 2014)

$$\mathcal{P}_+ = \mathcal{P}_{cons} = \mathcal{P}_-$$

Remark

When $p \equiv 1 \pmod 3$, primitive 3rd and 6th roots of unity modulo p^2 are always consecutive. If we prohibit those from counting towards $\mathcal{P}_{cons}$, and we also prohibit "resultant divisibilities" from counting towards $\mathcal{P}_+$ and $\mathcal{P}_-$, then the theorem also holds for the more restrictive sets of primes.

A polynomial for every prime

Definition

The roots of $f_p(x) = \dfrac{(x+1)^p - x^p - 1}{p} \in \mathbb{Z}[x]$ correspond exactly to consecutive pth powers modulo p^2.

- -1, 0, primitive 6th roots of unity always (trivial) roots
- $f_{59}(3) = 0$
- $f_p(1) = 0$ for Wieferich primes p

Hidden symmetry

It turns out that the nontrivial (and non-Wieferich) roots of $f_p(x)$ always come in *six-packs*

$$\left\{ x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x} \right\}.$$

A polynomial for every prime

Definition

The roots of $f_p(x) = \dfrac{(x+1)^p - x^p - 1}{p} \in \mathbb{Z}[x]$ correspond exactly to consecutive pth powers modulo p^2.

- -1, 0, primitive 6th roots of unity always (trivial) roots
- $f_{59}(3) = 0$
- $f_p(1) = 0$ for Wieferich primes p

Hidden symmetry

It turns out that the nontrivial (and non-Wieferich) roots of $f_p(x)$ always come in *six-packs*

$$\left\{ x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x} \right\}.$$

A polynomial for every prime

Definition

The roots of $f_p(x) = \dfrac{(x+1)^p - x^p - 1}{p} \in \mathbb{Z}[x]$ correspond exactly to consecutive pth powers modulo p^2.

- -1, 0, primitive 6th roots of unity always (trivial) roots
- $f_{59}(3) = 0$
- $f_p(1) = 0$ for Wieferich primes p

Hidden symmetry

It turns out that the nontrivial (and non-Wieferich) roots of $f_p(x)$ always come in *six-packs*

$$\left\{x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x}\right\}.$$

A polynomial for every prime

Definition

The roots of $f_p(x) = \dfrac{(x+1)^p - x^p - 1}{p} \in \mathbb{Z}[x]$ correspond exactly to consecutive pth powers modulo p^2.

- -1, 0, primitive 6th roots of unity always (trivial) roots
- $f_{59}(3) = 0$
- $f_p(1) = 0$ for Wieferich primes p

Hidden symmetry

It turns out that the nontrivial (and non-Wieferich) roots of $f_p(x)$ always come in *six-packs*

$$\left\{ x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x} \right\}.$$

A polynomial for every prime

Definition

The roots of $f_p(x) = \dfrac{(x+1)^p - x^p - 1}{p} \in \mathbb{Z}[x]$ correspond exactly to consecutive pth powers modulo p^2.

- -1, 0, primitive 6th roots of unity always (trivial) roots
- $f_{59}(3) = 0$
- $f_p(1) = 0$ for Wieferich primes p

Hidden symmetry

It turns out that the nontrivial (and non-Wieferich) roots of $f_p(x)$ always come in *six-packs*

$$\left\{ x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x} \right\}.$$

An impossible conjecture

There are approximately $p/6$ six-packs. If we assume that each six-pack has a probability of $1/p$ of having roots of f_p, then the probability of p *not* being in (the more restrictive) $\mathcal{P}_{cons}$ is

$$\approx \left(1 - \frac{1}{p}\right)^{p/6}.$$

Conjecture (Boyd, M., Thom)

$\mathcal{P}_{cons}$, the set of primes p for which there are two nontrivial consecutive pth powers modulo p^2, has relative density $1 - e^{-1/6} \approx 0.15352$ within the set of all primes.

In fact, the number of six-packs of roots of f_p should follow a Poisson distribution with parameter $\lambda = \frac{1}{6}$.

An impossible conjecture

There are approximately $p/6$ six-packs. If we assume that each six-pack has a probability of $1/p$ of having roots of f_p, then the probability of p *not* being in (the more restrictive) $\mathcal{P}_{cons}$ is

$$\approx \left(1 - \frac{1}{p}\right)^{p/6}.$$

Conjecture (Boyd, M., Thom)

$\mathcal{P}_{cons}$, the set of primes p for which there are two nontrivial consecutive pth powers modulo p^2, has relative density $1 - e^{-1/6} \approx 0.15352$ within the set of all primes.

In fact, the number of six-packs of roots of f_p should follow a Poisson distribution with parameter $\lambda = \frac{1}{6}$.

An impossible conjecture

There are approximately $p/6$ six-packs. If we assume that each six-pack has a probability of $1/p$ of having roots of f_p, then the probability of p *not* being in (the more restrictive) $\mathcal{P}_{cons}$ is

$$\approx \left(1 - \frac{1}{p}\right)^{p/6}.$$

Conjecture (Boyd, M., Thom)

$\mathcal{P}_{cons}$, the set of primes p for which there are two nontrivial consecutive pth powers modulo p^2, has relative density $1 - e^{-1/6} \approx 0.15352$ within the set of all primes.

In fact, the number of six-packs of roots of f_p should follow a Poisson distribution with parameter $\lambda = \frac{1}{6}$.

Testing the conjecture against reality

Definition

In a Poisson distribution with parameter $\frac{1}{6}$, the probability of k successes is $\frac{1}{k!}\left(\frac{1}{6}\right)^k e^{-1/6}$.

number (k) of six-packs	predicted frequency of f_p having exactly k six-packs of roots	predicted # of primes $3 \le p < 10^6$	actual # of primes $3 \le p < 10^6$
0	$e^{-1/6} \approx 84.6\%$	66,446.2	66,704
1	$\frac{1}{6}e^{-1/6} \approx 14.2\%$	11,074.4	10,833
2	$\frac{1}{72}e^{-1/6} \approx 1.18\%$	922.8	910
3	$\frac{1}{1296}e^{-1/6} \approx 0.066\%$	51.2	48
≥ 4	$\approx 0.0056\%$	4.4	2

Testing the conjecture against reality

Definition

In a Poisson distribution with parameter $\frac{1}{6}$, the probability of k successes is $\frac{1}{k!}\left(\frac{1}{6}\right)^k e^{-1/6}$.

number (k) of six-packs	predicted frequency of f_p having exactly k six-packs of roots	predicted # of primes $3 \le p < 10^6$	actual # of primes $3 \le p < 10^6$
0	$e^{-1/6} \approx 84.6\%$	66,446.2	66,704
1	$\frac{1}{6}e^{-1/6} \approx 14.2\%$	11,074.4	10,833
2	$\frac{1}{72}e^{-1/6} \approx 1.18\%$	922.8	910
3	$\frac{1}{1296}e^{-1/6} \approx 0.066\%$	51.2	48
≥ 4	$\approx 0.0056\%$	4.4	2

Back to squarefree values of $n^n + (-1)^n(n-1)^{n-1}$

Example

Given $59^2 \mid (257^{257} - 256^{256})$, it's easy to show that $59^2 \mid (n^n - (n-1)^{n-1})$ for any $n \equiv 257 \pmod{59 \cdot 58}$. So a positive proportion of values are *not* squarefree.

Other numerical examples show that a positive proportion of $n^n + (-1)^n(n-1)^{n-1}$ are not squarefree.

Conjecture (Boyd, M., Thom)

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree for $99.34466\ldots\%$ of positive integers n.

Although we can't even gather 100 data points, we still believe that proportion is accurate to the listed seven significant figures!

Back to squarefree values of $n^n + (-1)^n(n-1)^{n-1}$

Example

Given $59^2 \mid (257^{257} - 256^{256})$, it's easy to show that $59^2 \mid (n^n - (n-1)^{n-1})$ for any $n \equiv 257 \pmod{59 \cdot 58}$. So a positive proportion of values are *not* squarefree.

Other numerical examples show that a positive proportion of $n^n + (-1)^n(n-1)^{n-1}$ are not squarefree.

Conjecture (Boyd, M., Thom)

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree for $99.34466\ldots\%$ of positive integers n.

Although we can't even gather 100 data points, we still believe that proportion is accurate to the listed seven significant figures!

Back to squarefree values of $n^n + (-1)^n(n-1)^{n-1}$

Example

Given $59^2 \mid (257^{257} - 256^{256})$, it's easy to show that $59^2 \mid (n^n - (n-1)^{n-1})$ for any $n \equiv 257 \pmod{59 \cdot 58}$. So a positive proportion of values are *not* squarefree.

Other numerical examples show that a positive proportion of $n^n + (-1)^n(n-1)^{n-1}$ are not squarefree.

Conjecture (Boyd, M., Thom)

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree for $99.34466\ldots\%$ of positive integers n.

Although we can't even gather 100 data points, we still believe that proportion is accurate to the listed seven significant figures!

Back to squarefree values of $n^n + (-1)^n(n-1)^{n-1}$

Example

Given $59^2 \mid (257^{257} - 256^{256})$, it's easy to show that $59^2 \mid (n^n - (n-1)^{n-1})$ for any $n \equiv 257 \pmod{59 \cdot 58}$. So a positive proportion of values are *not* squarefree.

Other numerical examples show that a positive proportion of $n^n + (-1)^n(n-1)^{n-1}$ are not squarefree.

Conjecture (Boyd, M., Thom)

$n^n + (-1)^n(n-1)^{n-1}$ is squarefree for $99.34466\ldots\%$ of positive integers n.

Although we can't even gather 100 data points, we still believe that proportion is accurate to the listed seven significant figures!

Why should you believe us?

- Our proof that $\mathcal{P}_\pm = \mathcal{P}_{cons}$ comes with an explicit bjection between roots of f_p and residue classes $n \pmod{p(p-1)}$ for which p^2 divides $n^n \pm (n-1)^{n-1}$.
- With our collection of numerical examples of square divisors (with $p < 10^6$), we can prove an upper bound of 99.344674% for the percentage of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree.
- Then conjecture about frequency of primes in $\mathcal{P}_{cons} = \mathcal{P}_\pm$, together with heuristics about how many residue classes each such prime generates, shows that the other primes should contribute about $-\sum_{p>10^6} 1/p(p-1) \approx -7 \times 10^{-8}$.

Why should you believe us?

- Our proof that $\mathcal{P}_\pm = \mathcal{P}_{cons}$ comes with an explicit bjection between roots of f_p and residue classes $n \pmod{p(p-1)}$ for which p^2 divides $n^n \pm (n-1)^{n-1}$.
- With our collection of numerical examples of square divisors (with $p < 10^6$), we can prove an upper bound of 99.344674% for the percentage of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree.
- Then conjecture about frequency of primes in $\mathcal{P}_{cons} = \mathcal{P}_\pm$, together with heuristics about how many residue classes each such prime generates, shows that the other primes should contribute about $-\sum_{p>10^6} 1/p(p-1) \approx -7 \times 10^{-8}$.

Why should you believe us?

- Our proof that $\mathcal{P}_{\pm} = \mathcal{P}_{cons}$ comes with an explicit bjection between roots of f_p and residue classes $n \pmod{p(p-1)}$ for which p^2 divides $n^n \pm (n-1)^{n-1}$.
- With our collection of numerical examples of square divisors (with $p < 10^6$), we can prove an upper bound of 99.344674% for the percentage of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree.
- Then conjecture about frequency of primes in $\mathcal{P}_{cons} = \mathcal{P}_{\pm}$, together with heuristics about how many residue classes each such prime generates, shows that the other primes should contribute about $-\sum_{p>10^6} 1/p(p-1) \approx -7 \times 10^{-8}$.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n (n-1)^{n-1}$ is squarefree

Proving things must feel nice ...

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

$\mathcal{P}_{cons}$ (primes with consecutive pth powers modulo p^2)

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

$\mathcal{P}_{cons}$ (primes with consecutive pth powers modulo p^2)

- We can't prove that $\mathcal{P}_{cons}$ has density $1 - e^{-1/6}$.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

$\mathcal{P}_{cons}$ (primes with consecutive pth powers modulo p^2)

- We can't prove that $\mathcal{P}_{cons}$ has density $1 - e^{-1/6}$.
- We can't prove there are infinitely many primes in $\mathcal{P}_{cons}$.

Proving things must feel nice . . .

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

$\mathcal{P}_{cons}$ (primes with consecutive pth powers modulo p^2)

- We can't prove that $\mathcal{P}_{cons}$ has density $1 - e^{-1/6}$.
- We can't prove there are infinitely many primes in $\mathcal{P}_{cons}$.
- We can't prove there are infinitely many primes *not* in $\mathcal{P}_{cons}$. (We can't even prove there are infinitely many non-Wieferich primes.)

Proving things must feel nice ...

Proportion of n for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree

- We can't prove a lower bound close to 99.344674%.
- We can't prove any positive lower bound.
- We can't even prove that infinitely many of them are squarefree.

$\mathcal{P}_{cons}$ (primes with consecutive pth powers modulo p^2)

- We can't prove that $\mathcal{P}_{cons}$ has density $1 - e^{-1/6}$.
- We can't prove there are infinitely many primes in $\mathcal{P}_{cons}$.
- We can't prove there are infinitely many primes *not* in $\mathcal{P}_{cons}$. (We can't even prove there are infinitely many non-Wieferich primes.)
- We *can* prove there are infinitely many primes.

A new family of ABC triples

Notation

$\mathrm{rad}(n)$ is the radical of n (the product of the distinct primes dividing n).

Recall

$$(12k^2+6k+1)^2 \quad \text{divides} \quad (6k+2)^{6k+2}-(6k+1)^{6k+1}.$$

Choose k so that $6k+2=2^m$, and set:

$$a = (6k+1)^{6k+1} = (2^m-1)^{2^m-1}$$

$$b = (6k+2)^{6k+2}-(6k+1)^{6k+1}$$

$$c = a+b = (6k+2)^{6k+2} = 2^{m2^m}$$

- $\mathrm{rad}(abc) = \mathrm{rad}(2^m-1)\cdot\mathrm{rad}(b)\cdot 2 \le \mathrm{rad}(b)(12k+2)$
- $\mathrm{rad}(b) \le b/(12k^2+6k+1)$

A new family of ABC triples

Notation

$\mathrm{rad}(n)$ is the radical of n (the product of the distinct primes dividing n).

Recall

$$(12k^2 + 6k + 1)^2 \quad \text{divides} \quad (6k+2)^{6k+2} - (6k+1)^{6k+1}.$$

Choose k so that $6k + 2 = 2^m$, and set:

$$a = (6k+1)^{6k+1} = (2^m - 1)^{2^m - 1}$$
$$b = (6k+2)^{6k+2} - (6k+1)^{6k+1}$$
$$c = a + b = (6k+2)^{6k+2} = 2^{m2^m}$$

- $\mathrm{rad}(abc) = \mathrm{rad}(2^m - 1) \cdot \mathrm{rad}(b) \cdot 2 \le \mathrm{rad}(b)(12k+2)$
- $\mathrm{rad}(b) \le b/(12k^2 + 6k + 1)$

A new family of ABC triples

Notation

$\mathrm{rad}(n)$ is the radical of n (the product of the distinct primes dividing n).

Recall

$$(12k^2+6k+1)^2 \quad \text{divides} \quad (6k+2)^{6k+2}-(6k+1)^{6k+1}.$$

Choose k so that $6k+2=2^m$, and set:

$$a = (6k+1)^{6k+1} = (2^m-1)^{2^m-1}$$
$$b = (6k+2)^{6k+2}-(6k+1)^{6k+1}$$
$$c = a+b = (6k+2)^{6k+2} = 2^{m2^m}$$

- $\mathrm{rad}(abc) = \mathrm{rad}(2^m-1)\cdot\mathrm{rad}(b)\cdot 2 \le \mathrm{rad}(b)(12k+2)$
- $\mathrm{rad}(b) \le b/(12k^2+6k+1)$

A new family of ABC triples

Notation

$\mathrm{rad}(n)$ is the radical of n (the product of the distinct primes dividing n).

Recall

$$(12k^2+6k+1)^2 \quad \text{divides} \quad (6k+2)^{6k+2}-(6k+1)^{6k+1}.$$

Choose k so that $6k+2=2^m$, and set:

$$a = (6k+1)^{6k+1} = (2^m-1)^{2^m-1}$$
$$b = (6k+2)^{6k+2}-(6k+1)^{6k+1}$$
$$c = a+b = (6k+2)^{6k+2} = 2^{m2^m}$$

- $\mathrm{rad}(abc) = \mathrm{rad}(2^m-1)\cdot\mathrm{rad}(b)\cdot 2 \le \mathrm{rad}(b)(12k+2)$
- $\mathrm{rad}(b) \le b/(12k^2+6k+1)$

How good do these ABC triples do?

On the previous slide, we just used $\mathrm{rad}(2^m - 1) \le 2^m - 1$. But if m has lots of $p(p-1)$ factors, then lots of p^2 divide $2^m - 1$.

Folklore theorem

Let $(a, b, c) = (1, 2^m - 1, 2^m)$. There are infinitely many values of m for which $\mathrm{rad}(abc) \ll c/\log c$.

We need m odd, so that $2^m \equiv 2 \pmod 6$. But if $p \equiv 7 \pmod 8$ and $p(p-1)/2$ divides m, then p^2 again divides $2^m - 1$.

Theorem (Boyd, M., Thom)

$(a, b, c) = ((6k+1)^{6k+1}, (6k+2)^{6k+2} - (6k+1)^{6k+1}, (6k+2)^{6k+2})$

There are infinitely many values of k for which

$$\mathrm{rad}(abc) < \frac{c(\log\log c)^{3/4+o(1)}}{\log c}.$$

How good do these ABC triples do?

On the previous slide, we just used $\mathrm{rad}(2^m - 1) \le 2^m - 1$. But if m has lots of $p(p-1)$ factors, then lots of p^2 divide $2^m - 1$.

Folklore theorem

Let $(a, b, c) = (1, 2^m - 1, 2^m)$. There are infinitely many values of m for which $\mathrm{rad}(abc) \ll c/\log c$.

We need m odd, so that $2^m \equiv 2 \pmod 6$. But if $p \equiv 7 \pmod 8$ and $p(p-1)/2$ divides m, then p^2 again divides $2^m - 1$.

Theorem (Boyd, M., Thom)

$(a, b, c) = ((6k+1)^{6k+1}, (6k+2)^{6k+2} - (6k+1)^{6k+1}, (6k+2)^{6k+2})$

There are infinitely many values of k for which

$$\mathrm{rad}(abc) < \frac{c(\log\log c)^{3/4+o(1)}}{\log c}.$$

How good do these ABC triples do?

On the previous slide, we just used $\mathrm{rad}(2^m - 1) \le 2^m - 1$. But if m has lots of $p(p-1)$ factors, then lots of p^2 divide $2^m - 1$.

Folklore theorem

Let $(a, b, c) = (1, 2^m - 1, 2^m)$. There are infinitely many values of m for which $\mathrm{rad}(abc) \ll c/\log c$.

We need m odd, so that $2^m \equiv 2 \pmod 6$. But if $p \equiv 7 \pmod 8$ and $p(p-1)/2$ divides m, then p^2 again divides $2^m - 1$.

Theorem (Boyd, M., Thom)

$(a, b, c) = ((6k+1)^{6k+1}, (6k+2)^{6k+2} - (6k+1)^{6k+1}, (6k+2)^{6k+2})$

There are infinitely many values of k for which

$$\mathrm{rad}(abc) < \frac{c(\log\log c)^{3/4+o(1)}}{\log c}.$$

How good do these ABC triples do?

On the previous slide, we just used $\mathrm{rad}(2^m - 1) \le 2^m - 1$. But if m has lots of $p(p-1)$ factors, then lots of p^2 divide $2^m - 1$.

Folklore theorem

Let $(a, b, c) = (1, 2^m - 1, 2^m)$. There are infinitely many values of m for which $\mathrm{rad}(abc) \ll c/\log c$.

We need m odd, so that $2^m \equiv 2 \pmod 6$. But if $p \equiv 7 \pmod 8$ and $p(p-1)/2$ divides m, then p^2 again divides $2^m - 1$.

Theorem (Boyd, M., Thom)

$(a, b, c) = ((6k+1)^{6k+1}, (6k+2)^{6k+2} - (6k+1)^{6k+1}, (6k+2)^{6k+2})$

There are infinitely many values of k for which

$$\mathrm{rad}(abc) < \frac{c(\log\log c)^{3/4+o(1)}}{\log c}.$$

The end

The paper *Squarefree values of trinomial discriminants* is currently still in progress; these slides are available for downloading.

The paper (soon)

www.math.ubc.ca/~gerg/
index.shtml?abstract=SFTD

These slides

www.math.ubc.ca/~gerg/index.shtml?slides