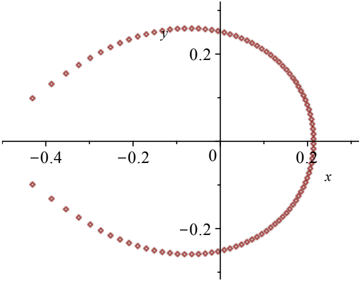
Some polynomial and geometric Diophantine equations

Karl Dilcher

Number Theory Seminar, March 11, 2019

Part I

Polynomial Diophantine Equations



Joint work with

Maciej Ulas
Jagiellonian University, Kraków, Poland

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

They can be defined by $T_0(x) = 1$, $T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

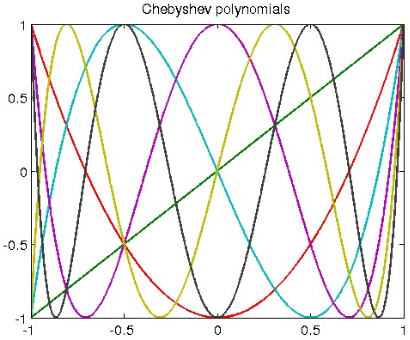
1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

They can be defined by $T_0(x) = 1$, $T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$



Similarly, Chebyshev polynomials of the second kind, $U_n(x)$, can be defined by $U_0(x) = 1$, $U_1(x) = 2x$, and

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x) \qquad (n \geq 1).$$

Similarly, Chebyshev polynomials of the second kind, $U_n(x)$, can be defined by $U_0(x) = 1$, $U_1(x) = 2x$, and

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x) \qquad (n \geq 1).$$

$T_n(x)$ and $U_n(x)$ can also be defined as solutions of the polynomial Pell equation

$$T_n(x)^2 - (x^2 - 1)U_{n-1}(x)^2 = 1$$

in the ring $\mathbb{Z}[x]$.

Similarly, Chebyshev polynomials of the second kind, $U_n(x)$, can be defined by $U_0(x) = 1$, $U_1(x) = 2x$, and

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x) \qquad (n \geq 1).$$

$T_n(x)$ and $U_n(x)$ can also be defined as solutions of the polynomial Pell equation

$$T_n(x)^2 - (x^2 - 1)U_{n-1}(x)^2 = 1$$

in the ring $\mathbb{Z}[x]$.

Here we'll consider a variant of this equation.

$\mathbb{Q}[x]$ is a Euclidean domain, so for given coprime $f, g \in \mathbb{Q}[x]$ there are $P, Q \in \mathbb{Q}[x]$ with

$$P(x)f(x) + Q(x)g(x) = 1.$$

$\mathbb{Q}[x]$ is a Euclidean domain, so for given coprime $f, g \in \mathbb{Q}[x]$ there are $P, Q \in \mathbb{Q}[x]$ with

$$P(x)f(x) + Q(x)g(x) = 1.$$

Choose f, g to be the simplest pair of coprime polynomials of the same degree, namely

$$x^{n+1} \quad \text{and} \quad (x+1)^{n+1}, \qquad (n \geq 0).$$

$\mathbb{Q}[x]$ is a Euclidean domain, so for given coprime $f, g \in \mathbb{Q}[x]$ there are $P, Q \in \mathbb{Q}[x]$ with

$$P(x)f(x) + Q(x)g(x) = 1.$$

Choose f, g to be the simplest pair of coprime polynomials of the same degree, namely

$$x^{n+1} \quad \text{and} \quad (x+1)^{n+1}, \qquad (n \geq 0).$$

If we assume that $\deg P \leq n$, $\deg Q \leq n$, then there is a unique solution $P(x) = P_n(x), Q(x) = Q_n(x)$.

$\mathbb{Q}[x]$ is a Euclidean domain, so for given coprime $f, g \in \mathbb{Q}[x]$ there are $P, Q \in \mathbb{Q}[x]$ with

$$P(x)f(x) + Q(x)g(x) = 1.$$

Choose f, g to be the simplest pair of coprime polynomials of the same degree, namely

$$x^{n+1} \quad \text{and} \quad (x+1)^{n+1}, \qquad (n \geq 0).$$

If we assume that $\deg P \leq n$, $\deg Q \leq n$, then there is a unique solution $P(x) = P_n(x), Q(x) = Q_n(x)$.

Purpose: To study the sequences $P_n(x), Q_n(x)$.

n	$P_n(x)$
0	-1
1	$2x+3$
2	$-6x^2-15x-10$
3	$20x^3+70x^2+84x+35$
4	$-70x^4-315x^3-540x^2-420x-126$

n	$Q_n(x)$
0	1
1	$-2x+1$
2	$6x^2-3x+1$
3	$-20x^3+10x^2-4x+1$
4	$70x^4-35x^3+15x^2-5x+1$

Table 1: $P_n(x)$ and $Q_n(x)$ for $0 \leq n \leq 4$.

2. Basic Properties

Proposition

For $n \geq 0$ we have $\deg P_n = \deg Q_n$, and

$$P_n(x) = (-1)^{n+1} Q_n(-1-x), \quad Q_n(x) = (-1)^{n+1} P_n(-1-x).$$

2. Basic Properties

Proposition

For $n \geq 0$ we have $\deg P_n = \deg Q_n$, *and*

$$P_n(x) = (-1)^{n+1} Q_n(-1-x), \quad Q_n(x) = (-1)^{n+1} P_n(-1-x).$$

Proof: Replace x by $-1-x$ and use uniqueness.

2. Basic Properties

Proposition

For $n \geq 0$ *we have* $\deg P_n = \deg Q_n$*, and*

$$P_n(x) = (-1)^{n+1} Q_n(-1-x), \quad Q_n(x) = (-1)^{n+1} P_n(-1-x).$$

Proof: Replace x by $-1-x$ and use uniqueness.

Corollary

$$P_n(-1) = (-1)^{n+1}, \quad P_n(-\tfrac{1}{2}) = (-1)^{n+1} 2^n,$$
$$Q_n(-\tfrac{1}{2}) = 2^n, \quad Q_n(0) = 1.$$

2. Basic Properties

Proposition

For $n \geq 0$ we have $\deg P_n = \deg Q_n$, *and*

$$P_n(x) = (-1)^{n+1} Q_n(-1-x), \quad Q_n(x) = (-1)^{n+1} P_n(-1-x).$$

Proof: Replace x by $-1-x$ and use uniqueness.

Corollary

$$P_n(-1) = (-1)^{n+1}, \quad P_n(-\tfrac{1}{2}) = (-1)^{n+1} 2^n,$$
$$Q_n(-\tfrac{1}{2}) = 2^n, \quad Q_n(0) = 1.$$

Proof: In $P_n(x)x^{n+1} + Q_n(x)(x+1)^{n+1} = 1$, set $x = 0, -1$, and $-1/2$.

Explicit formulas:

Proposition

For any $n \geq 0$ *we have* $\deg Q_n = degP_n = n$*, and*

$$Q_n(x) = \sum_{i=0}^{n} (-1)^i \binom{n+i}{i} x^i, \qquad (1)$$

Explicit formulas:

Proposition

For any $n \geq 0$ we have $\deg Q_n = degP_n = n$, and

$$Q_n(x) = \sum_{i=0}^{n} (-1)^i \binom{n+i}{i} x^i, \tag{1}$$

$$P_n(x) = (-1)^{n+1}(2n+1)\binom{2n}{n} \sum_{i=0}^{n} \frac{1}{n+i+1} \binom{n}{i} x^i. \tag{2}$$

Explicit formulas:

Proposition

For any $n \geq 0$ we have $\deg Q_n = degP_n = n$*, and*

$$Q_n(x) = \sum_{i=0}^{n} (-1)^i \binom{n+i}{i} x^i, \tag{1}$$

$$P_n(x) = (-1)^{n+1}(2n+1)\binom{2n}{n} \sum_{i=0}^{n} \frac{1}{n+i+1} \binom{n}{i} x^i. \tag{2}$$

Idea of Proof: For (1):

- Differentiate $P_n(x)x^{n+1} + Q_n(x)(x+1)^{n+1} = 1$;
- make some divisibility arguments;
- use induction.

Explicit formulas:

Proposition

For any $n \geq 0$ *we have* $\deg Q_n = deg P_n = n$*, and*

$$Q_n(x) = \sum_{i=0}^{n} (-1)^i \binom{n+i}{i} x^i, \tag{1}$$

$$P_n(x) = (-1)^{n+1}(2n+1)\binom{2n}{n} \sum_{i=0}^{n} \frac{1}{n+i+1} \binom{n}{i} x^i. \tag{2}$$

Idea of Proof: For (1):

- Differentiate $P_n(x)x^{n+1} + Q_n(x)(x+1)^{n+1} = 1$;
- make some divisibility arguments;
- use induction.

For (2): Use (1) and $P_n(x) = (-1)^{n+1} Q_n(-1-x)$.

Proposition

For $1 \leq k \leq n+1$ *we have*

$$(x+1)Q_n^{(k)}(x)+(n+k)Q_n^{(k-1)}(x) = (-1)^n\frac{(2n+1)!}{n!}\frac{x^{n-k+1}}{(n-k+1)!},$$

Proposition

For $1 \leq k \leq n+1$ *we have*

$$(x+1)Q_n^{(k)}(x)+(n+k)Q_n^{(k-1)}(x) = (-1)^n \frac{(2n+1)!}{n!} \frac{x^{n-k+1}}{(n-k+1)!},$$

and in particular

$$(x+1)Q_n'(x) + (n+1)Q_n(x) = (-1)^n(2n+1)\binom{2n}{n}x^n.$$

Proposition

For $1 \leq k \leq n+1$ *we have*

$$(x+1)Q_n^{(k)}(x)+(n+k)Q_n^{(k-1)}(x) = (-1)^n\frac{(2n+1)!}{n!}\frac{x^{n-k+1}}{(n-k+1)!},$$

and in particular

$$(x+1)Q_n'(x)+(n+1)Q_n(x) = (-1)^n(2n+1)\binom{2n}{n}x^n.$$

Homogeneous ODE:

Corollary

For $n \geq 0$ *we have*

$$x(x+1)Q_n''(x)+(2x-n)Q_n'(x)-n(n+1)Q_n(x)=0.$$

Recurrence relation:

Proposition

$Q_0(x) = 1$ and $Q_1(x) = -2x + 1$, and for $n \geq 2$,

$$n(x+1)Q_n(x) = -\big(2(2n-1)x^2 + 2(2n-1)x - n\big)Q_{n-1}(x) \\ + 2(2n-1)xQ_{n-2}(x).$$

Recurrence relation:

Proposition

$Q_0(x) = 1$ and $Q_1(x) = -2x + 1$, and for $n \geq 2$,

$$n(x+1)Q_n(x) = -\big(2(2n-1)x^2 + 2(2n-1)x - n\big)Q_{n-1}(x) \\ + 2(2n-1)xQ_{n-2}(x).$$

Proof: Apply D. Zeilberger's Maple package `EKHAD` to the explicit formula. (Can also be verified by direct computation with the explicit formula).

Recurrence relation:

Proposition

$Q_0(x) = 1$ and $Q_1(x) = -2x + 1$, and for $n \geq 2$,

$$n(x+1)Q_n(x) = -\big(2(2n-1)x^2 + 2(2n-1)x - n\big)Q_{n-1}(x) + 2(2n-1)xQ_{n-2}(x).$$

Proof: Apply D. Zeilberger's Maple package `EKHAD` to the explicit formula. (Can also be verified by direct computation with the explicit formula).

Consequence: Generating function.

Corollary

$$\frac{1 + xt + (1+2x)\sqrt{1+4xt}}{2(1+x-t)(1+4xt)} = \sum_{n=0}^{\infty} Q_n(x)t^n.$$

3. Resultants

Suppose we have the two polynomials

$$f(x) = a_0 x^\mu + \cdots + a_{\mu-1} x + a_\mu = a_0(x - \alpha_1)\cdots(x - \alpha_\mu),$$
$$g(x) = b_0 x^m + \cdots + b_{m-1} x + b_m = b_0(x - \beta_1)\cdots(x - \beta_m).$$

3. Resultants

Suppose we have the two polynomials

$$f(x) = a_0 x^\mu + \cdots + a_{\mu-1} x + a_\mu = a_0(x-\alpha_1)\cdots(x-\alpha_\mu),$$
$$g(x) = b_0 x^m + \cdots + b_{m-1} x + b_m = b_0(x-\beta_1)\cdots(x-\beta_m).$$

Recall: The resultant of f and g with respect to x can be defined by

$$R(f,g) = a_0^m b_0^\mu \prod_{\substack{1\le i\le m\\ 1\le j\le \mu}} \left(\beta_j - \alpha_i\right).$$

3. Resultants

Suppose we have the two polynomials

$$f(x) = a_0 x^\mu + \cdots + a_{\mu-1}x + a_\mu = a_0(x-\alpha_1)\cdots(x-\alpha_\mu),$$
$$g(x) = b_0 x^m + \cdots + b_{m-1}x + b_m = b_0(x-\beta_1)\cdots(x-\beta_m).$$

Recall: The resultant of f and g with respect to x can be defined by

$$R(f,g) = a_0^m b_0^\mu \prod_{\substack{1\le i\le m\\ 1\le j\le \mu}} \left(\beta_j - \alpha_i\right).$$

Some properties:

$$R(f,g) = a_0^m \prod_{i=1}^{\mu} g(\alpha_i),$$
$$R(f,g) = (-1)^{\mu m} R(g,f),$$
$$R(f,pq) = R(f,p)\cdot R(f,q),$$

Another useful property:

Lemma

If we can write

$$f(x) = q(x)g(x) + r(x)$$

with polynomials q, r *and* $\nu := \deg r$*, then*

$$R(g, f) = b_0^{\mu-\nu} R(g, r).$$

Another useful property:

Lemma

If we can write

$$f(x) = q(x)g(x) + r(x)$$

with polynomials q, r *and* $\nu := \deg r$, *then*

$$R(g, f) = b_0^{\mu-\nu} R(g, r).$$

With these properties we can prove:

Theorem

For any integer $n \geq 1$ *we have*

$$R(Q_n(x), Q_{n-1}(x)) = 2^n \binom{2n}{n}^{n-2}.$$

A result that is similar in nature:

Theorem

For any $n \geq 0$ we have

$$R(P_n(x), Q_n(x)) = \binom{2n}{n}^{n+1}.$$

A result that is similar in nature:

Theorem

For any $n \geq 0$ we have

$$R(P_n(x), Q_n(x)) = \binom{2n}{n}^{n+1}.$$

For the proof we rewrite the defining equation as

$$P_n(x)x^{n+1} = -(x+1)^{n+1}Q_n(x) + 1,$$

and use explicit formlas (in particular the leading coefficients) and the above properties.

4. Discriminants

Recall: Given a polynomial

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_1 x + a_0 \\ &= a_m (x - \theta_1) \cdots (x - \theta_m), \end{aligned}$$

$(a_m \neq 0)$, the discriminant of f is defined by

$$\begin{aligned} \mathrm{Disc}(f) &= (-1)^{\frac{m(m-1)}{2}} a_m^{-1} R(f, f') \\ &= (-1)^{\frac{m(m-1)}{2}} a_m^{m-2} \prod_{i=1}^{m} f'(\theta_i). \end{aligned}$$

4. Discriminants

Recall: Given a polynomial

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_1 x + a_0 \\ &= a_m (x-\theta_1)\cdots(x-\theta_m), \end{aligned}$$

($a_m \neq 0$), the discriminant of f is defined by

$$\begin{aligned} \mathrm{Disc}(f) &= (-1)^{\frac{m(m-1)}{2}} a_m^{-1} R(f, f') \\ &= (-1)^{\frac{m(m-1)}{2}} a_m^{m-2} \prod_{i=1}^{m} f'(\theta_i). \end{aligned}$$

It follows that $\mathrm{Disc}(f) = 0$ iff f has multiple roots.

Theorem

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(Q_n^{(k)}(x)) = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1},$$

where $\varepsilon := (n-k)(n-k-1)/2$.

Theorem

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(Q_n^{(k)}(x)) = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1},$$

where $\varepsilon := (n-k)(n-k-1)/2$. In particular, for $n \geq 1$,

$$\mathrm{Disc}(Q_n(x)) = (-1)^{\frac{n(n-1)}{2}} (n+1)(2n+1)^{n-1} \binom{2n}{n}^{n-2}.$$

Theorem

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(Q_n^{(k)}(x)) = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1},$$

where $\varepsilon := (n-k)(n-k-1)/2$*. In particular, for* $n \geq 1$*,*

$$\mathrm{Disc}(Q_n(x)) = (-1)^{\frac{n(n-1)}{2}} (n+1)(2n+1)^{n-1} \binom{2n}{n}^{n-2}.$$

Main ingredient in proof:

$$(x+1)Q_n^{(k+1)}(x) + (n+k+1)Q_n^{(k)}(x) = (-1)^n \frac{(2n+1)!}{n!} \frac{x^{n-k}}{(n-k)!}.$$

Let x run through the zeros of $Q_n^{(k)}(x)$; use product identity for the discriminant.

Corollary

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(P_n^{(k)}(x)) = \mathrm{Disc}(Q_n^{(k)}(x)).$$

Corollary

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(P_n^{(k)}(x)) = \mathrm{Disc}(Q_n^{(k)}(x)).$$

This follows from $P_n^{(k)}(x) = (-1)^{n+k+1} Q_n^{(k)}(-x-1)$ and the discriminant identities

$$\mathrm{Disc}(f(ax+b)) = a^{m(m-1)}\mathrm{Disc}(f(x)),$$
$$\mathrm{Disc}(cf(x)) = c^{2(m-1)}\mathrm{Disc}(f(x)).$$

Corollary

For integers $n > k \geq 0$ we have

$$\mathrm{Disc}(P_n^{(k)}(x)) = \mathrm{Disc}(Q_n^{(k)}(x)).$$

This follows from $P_n^{(k)}(x) = (-1)^{n+k+1} Q_n^{(k)}(-x-1)$ and the discriminant identities

$$\mathrm{Disc}(f(ax+b)) = a^{m(m-1)}\mathrm{Disc}(f(x)),$$
$$\mathrm{Disc}(cf(x)) = c^{2(m-1)}\mathrm{Disc}(f(x)).$$

Remark: Compare with the Chebyshev polynomials:

$$\mathrm{Disc}(T_n(x)) = 2^{(n-1)^2} n^n,$$
$$\mathrm{Disc}(U_n(x)) = 2^{n^2}(n+1)^{n-2}.$$

Why are we interested in discriminants?

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Question: Can the discriminant of $Q_n^{(k)}(x)$ be a square?

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Question: Can the discriminant of $Q_n^{(k)}(x)$ be a square?

Computations show: $\mathrm{Disc}(Q_n)$ is a square when $n = 1, 24, 840, 28560$.

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Question: Can the discriminant of $Q_n^{(k)}(x)$ be a square?

Computations show: $\mathrm{Disc}(Q_n)$ is a square when $n = 1, 24, 840, 28560$.

- Are there more?

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Question: Can the discriminant of $Q_n^{(k)}(x)$ be a square?

Computations show: $\mathrm{Disc}(Q_n)$ is a square when $n = 1, 24, 840, 28560$.

- Are there more?
- How can we characterize them?

Why are we interested in discriminants?

Knowledge of the discriminant of a polynomial is often important for determining the polynomial's Galois group.

In particular, it is known that if the discriminant is the square of a nonzero integer, then the Galois group is a subgroup of the alternating group A_n.

Question: Can the discriminant of $Q_n^{(k)}(x)$ be a square?

Computations show: $\mathrm{Disc}(Q_n)$ is a square when $n = 1, 24, 840, 28560$.

- Are there more?
- How can we characterize them?
- How about $\mathrm{Disc}(Q_n^{(k)})$ for $k \geq 1$?

Let $n > k \geq 0$, and set $D_{k,n} := \mathrm{Disc}(Q_n^{(k)})$.

Corollary

(a) If $n \equiv k+2$ or $k+3 \pmod 4$, then $D_{k,n}$ is not the square of an integer.

Let $n > k \geq 0$, and set $D_{k,n} := \mathrm{Disc}(Q_n^{(k)})$.

Corollary

(*a*) *If* $n \equiv k + 2$ *or* $k + 3 \pmod 4$, *then* $D_{k,n}$ *is not the square of an integer.*

(*b*) *If* $n \equiv k + 1 \pmod 4$, *then for a given* k, $D_{k,n}$ *is a square for at most finitely many* n.

Let $n > k \geq 0$, and set $D_{k,n} := \mathrm{Disc}(Q_n^{(k)})$.

Corollary

(a) *If $n \equiv k+2$ or $k+3 \pmod 4$, then $D_{k,n}$ is not the square of an integer.*

(b) *If $n \equiv k+1 \pmod 4$, then for a given k, $D_{k,n}$ is a square for at most finitely many n.*

(c) *If $n \equiv k \pmod 4$, then for each k there are infinitely many n such that $D_{k,n}$ is a square.*

Let $n > k \geq 0$, and set $D_{k,n} := \mathrm{Disc}(Q_n^{(k)})$.

Corollary

(a) *If* $n \equiv k+2$ *or* $k+3 \pmod 4$*, then* $D_{k,n}$ *is not the square of an integer.*

(b) *If* $n \equiv k+1 \pmod 4$*, then for a given* k*,* $D_{k,n}$ *is a square for at most finitely many* n*.*

(c) *If* $n \equiv k \pmod 4$*, then for each* k *there are infinitely many* n *such that* $D_{k,n}$ *is a square.*

(d) *In particular,* $D_{0,n}$ *is a square if and only if* $n = 1$ *or* $n = n_j$*, where*

$$n_j := \frac{1}{8}\left((3+2\sqrt{2})^{2j+1} + (3-2\sqrt{2})^{2j+1} - 6\right), \qquad j = 1, 2, 3, \ldots$$

Let $n > k \geq 0$, and set $D_{k,n} := \mathrm{Disc}(Q_n^{(k)})$.

Corollary

(*a*) *If* $n \equiv k+2$ *or* $k+3 \pmod 4$, *then* $D_{k,n}$ *is not the square of an integer.*

(*b*) *If* $n \equiv k+1 \pmod 4$, *then for a given* k, $D_{k,n}$ *is a square for at most finitely many* n.

(*c*) *If* $n \equiv k \pmod 4$, *then for each* k *there are infinitely many* n *such that* $D_{k,n}$ *is a square.*

(*d*) *In particular,* $D_{0,n}$ *is a square if and only if* $n = 1$ *or* $n = n_j$, *where*

$$n_j := \frac{1}{8}\left((3+2\sqrt{2})^{2j+1} + (3-2\sqrt{2})^{2j+1} - 6\right), \qquad j = 1, 2, 3, \ldots$$

Remark: Part (d) shows that $D_{0,n}$ is a square for $n = 1, 24, 840, 28560, 970224, 32959080, 1119638520, 38034750624, \ldots$

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon}\frac{n+k+1}{\binom{2n}{n+k}}\left(\frac{(n+k)!}{(n-k)!}\binom{2n}{n}(2n+1)\right)^{n-k-1}.$$

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

(b) We can show: $D_{k,n}$ is a square iff $(n+k+2)(n+k+3)\cdots(2n-1)$ is.

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

(b) We can show: $D_{k,n}$ is a square iff
$(n+k+2)(n+k+3)\cdots(2n-1)$ is.

However, by the Prime Number Theorem: for a fixed k and for n sufficiently large, there is always a prime among the members of the sequence $n+k+2, n+k+3, \ldots, 2n-1$.

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

(b) We can show: $D_{k,n}$ is a square iff
$(n+k+2)(n+k+3)\cdots(2n-1)$ is.

However, by the Prime Number Theorem: for a fixed k and for n sufficiently large, there is always a prime among the members of the sequence $n+k+2, n+k+3, \ldots, 2n-1$.
(In fact, we can show that this is the case when $n > \frac{3}{2}(k+1)$.)

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon}\frac{n+k+1}{\binom{2n}{n+k}}\left(\frac{(n+k)!}{(n-k)!}\binom{2n}{n}(2n+1)\right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

(b) We can show: $D_{k,n}$ is a square iff
$(n+k+2)(n+k+3)\cdots(2n-1)$ is.

However, by the Prime Number Theorem: for a fixed k and for n sufficiently large, there is always a prime among the members of the sequence $n+k+2, n+k+3, \ldots, 2n-1$.
(In fact, we can show that this is the case when $n > \frac{3}{2}(k+1)$.)

This means the product cannot be a square.

Proof is based on the formula in the previous theorem:

$$D_{k,n} = (-1)^{\varepsilon} \frac{n+k+1}{\binom{2n}{n+k}} \left(\frac{(n+k)!}{(n-k)!} \binom{2n}{n} (2n+1) \right)^{n-k-1}.$$

(a) In this case, $D_{k,n} < 0$.

(b) We can show: $D_{k,n}$ is a square iff
$(n+k+2)(n+k+3)\cdots(2n-1)$ is.

However, by the Prime Number Theorem: for a fixed k and for n sufficiently large, there is always a prime among the members of the sequence $n+k+2, n+k+3, \ldots, 2n-1$.
(In fact, we can show that this is the case when $n > \frac{3}{2}(k+1)$.)

This means the product cannot be a square.

(c), (d) The condition for squareness can be reduced to a Pell-type equation, which has infinitely many solutions.

5. Distribution of Zeros

The nonvanishing of the discriminants implies:

Corollary

For $0 \le k \le n$ the polynomial $Q_n^{(k)}(x)$ has no multiple roots.

5. Distribution of Zeros

The nonvanishing of the discriminants implies:

Corollary

For $0 \le k \le n$ *the polynomial* $Q_n^{(k)}(x)$ *has no multiple roots.*

Recall: Chebyshev polynomials (and in fact all classical orthogonal polynomials) have only real roots. However:

5. Distribution of Zeros

The nonvanishing of the discriminants implies:

Corollary

For $0 \le k \le n$ the polynomial $Q_n^{(k)}(x)$ has no multiple roots.

Recall: Chebyshev polynomials (and in fact all classical orthogonal polynomials) have only real roots. However:

Theorem

For $0 \le k < n$ the polynomial $Q_n^{(k)}(x)$ has
(a) no real roots when $n \equiv k \pmod{2}$,

5. Distribution of Zeros

The nonvanishing of the discriminants implies:

Corollary

For $0 \le k \le n$ the polynomial $Q_n^{(k)}(x)$ has no multiple roots.

Recall: Chebyshev polynomials (and in fact all classical orthogonal polynomials) have only real roots. However:

Theorem

For $0 \le k < n$ the polynomial $Q_n^{(k)}(x)$ has
(a) no real roots when $n \equiv k \pmod 2$,
(b) exactly one positive real root when $n \not\equiv k \pmod 2$.

5. Distribution of Zeros

The nonvanishing of the discriminants implies:

Corollary

For $0 \le k \le n$ the polynomial $Q_n^{(k)}(x)$ has no multiple roots.

Recall: Chebyshev polynomials (and in fact all classical orthogonal polynomials) have only real roots. However:

Theorem

For $0 \le k < n$ the polynomial $Q_n^{(k)}(x)$ has
(a) no real roots when $n \equiv k \pmod 2$,
(b) exactly one positive real root when $n \not\equiv k \pmod 2$.

Proof is based on the connection between $Q_n^{(k)}(x)$ and $Q_n^{(k+1)}(x)$.

How, then, are the zeros distributed in $\mathbb{C}$?

How, then, are the zeros distributed in $\mathbb{C}$?
A preliminary result:

Theorem

For $0 \leq k < n$, all zeros of $Q_n^{(k)}(z)$ have modulus $|z| \leq \frac{1}{2}$.

How, then, are the zeros distributed in $\mathbb{C}$?
A preliminary result:

Theorem

For $0 \leq k < n$, all zeros of $Q_n^{(k)}(z)$ have modulus $|z| \leq \frac{1}{2}$.

Proof: From the explicit expression we get

$$Q_n^{(k)}(-\tfrac{z}{2}) = \frac{(-1)^k}{n!} \sum_{i=0}^{n-k} \frac{(n+k+i)!}{2^i i!} z^i.$$

How, then, are the zeros distributed in $\mathbb{C}$?
A preliminary result:

Theorem

For $0 \leq k < n$, all zeros of $Q_n^{(k)}(z)$ have modulus $|z| \leq \frac{1}{2}$.

Proof: From the explicit expression we get

$$Q_n^{(k)}(-\tfrac{z}{2}) = \frac{(-1)^k}{n!} \sum_{i=0}^{n-k} \frac{(n+k+i)!}{2^i i!} z^i.$$

We can show that the coefficients of z^i form an increasing sequence.

How, then, are the zeros distributed in $\mathbb{C}$?
A preliminary result:

Theorem

For $0 \le k < n$, all zeros of $Q_n^{(k)}(z)$ have modulus $|z| \le \frac{1}{2}$.

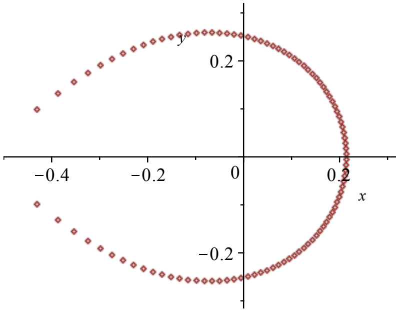
Proof: From the explicit expression we get

$$Q_n^{(k)}(-\tfrac{z}{2}) = \frac{(-1)^k}{n!}\sum_{i=0}^{n-k}\frac{(n+k+i)!}{2^i i!}z^i.$$

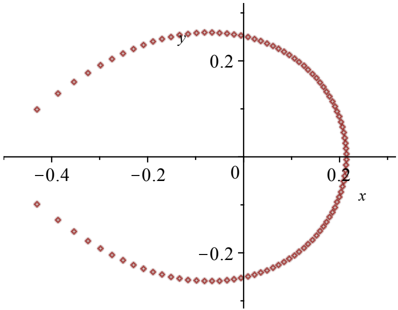
We can show that the coefficients of z^i form an increasing sequence.

The Eneström-Kakeya theorem can then be used.

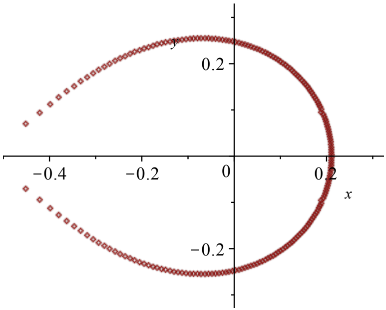
Plotting the zeros:



Plotting the zeros:

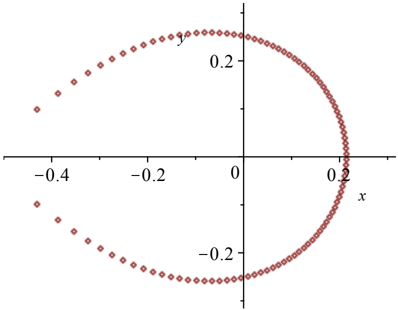


Zeros of $Q_{100}(x)$

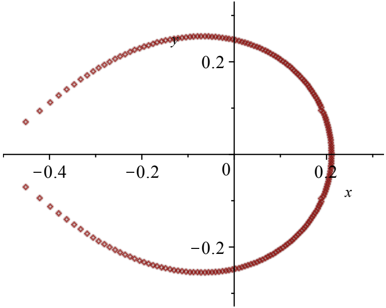


Zeros of $Q_{200}(x)$

Plotting the zeros:



Zeros of $Q_{100}(x)$



Zeros of $Q_{200}(x)$

Is there a limiting curve?

Theorem

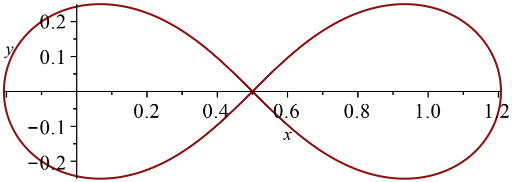
The zeros of $Q_n(-z)$ get arbitrarily close to the "half lemniscate"

$$\{z \in \mathbb{C} : |z(1-z)| = \tfrac{1}{4}\} \quad \cap \quad \{z \in \mathbb{C} : |z| \le \tfrac{1}{2}\}.$$

Theorem

The zeros of $Q_n(-z)$ get arbitrarily close to the "half lemniscate"

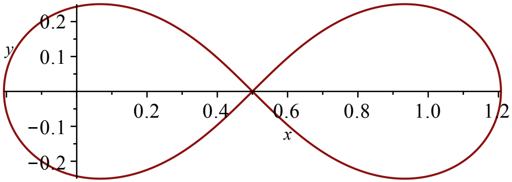
$$\{z \in \mathbb{C} : |z(1-z)| = \tfrac{1}{4}\} \quad \cap \quad \{z \in \mathbb{C} : |z| \le \tfrac{1}{2}\}.$$



Theorem

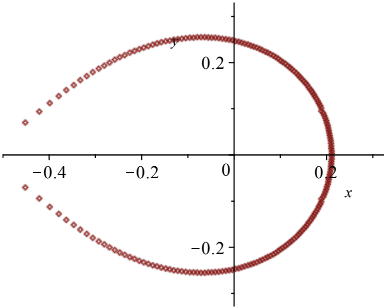
The zeros of $Q_n(-z)$ get arbitrarily close to the “half lemniscate"

$$\{z \in \mathbb{C} : |z(1-z)| = \tfrac{1}{4}\} \quad \cap \quad \{z \in \mathbb{C} : |z| \le \tfrac{1}{2}\}.$$

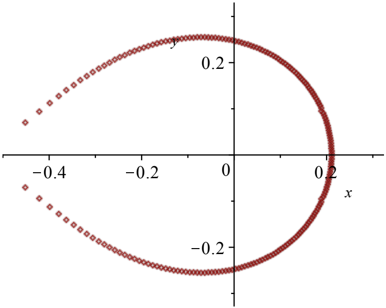


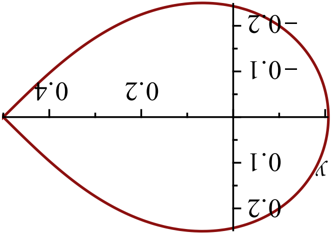
A special case of an Oval of Cassini

Compare:



Compare:





Idea of proof. From explicit formula:

$$Q_n(-z) = \sum_{j=0}^{n} \binom{n+j}{j} z^j.$$

Idea of proof. From explicit formula:

$$Q_n(-z) = \sum_{j=0}^{n} \binom{n+j}{j} z^j.$$

Well-known binomial identity:

$$\sum_{j=0}^{\infty} \binom{n+j}{j} z^j = \frac{1}{(1-z)^{n+1}},$$

Idea of proof. From explicit formula:

$$Q_n(-z) = \sum_{j=0}^{n} \binom{n+j}{j} z^j.$$

Well-known binomial identity:

$$\sum_{j=0}^{\infty} \binom{n+j}{j} z^j = \frac{1}{(1-z)^{n+1}},$$

and thus

$$Q_n(-z) = \frac{1}{(1-z)^{n+1}} - \sum_{j=n+1}^{\infty} \binom{n+j}{n} z^j.$$

Idea of proof. From explicit formula:

$$Q_n(-z) = \sum_{j=0}^{n} \binom{n+j}{j} z^j.$$

Well-known binomial identity:

$$\sum_{j=0}^{\infty} \binom{n+j}{j} z^j = \frac{1}{(1-z)^{n+1}},$$

and thus

$$Q_n(-z) = \frac{1}{(1-z)^{n+1}} - \sum_{j=n+1}^{\infty} \binom{n+j}{n} z^j.$$

Consequently,

$$\left|\frac{1}{z^{n+1}} Q_n(-z)\right| \geq \frac{1}{|z(1-z)|^{n+1}} - \sum_{j=0}^{\infty} \binom{2n+1+j}{n} |z|^j.$$

Idea of proof. From explicit formula:

$$Q_n(-z) = \sum_{j=0}^{n} \binom{n+j}{j} z^j.$$

Well-known binomial identity:

$$\sum_{j=0}^{\infty} \binom{n+j}{j} z^j = \frac{1}{(1-z)^{n+1}},$$

and thus

$$Q_n(-z) = \frac{1}{(1-z)^{n+1}} - \sum_{j=n+1}^{\infty} \binom{n+j}{n} z^j.$$

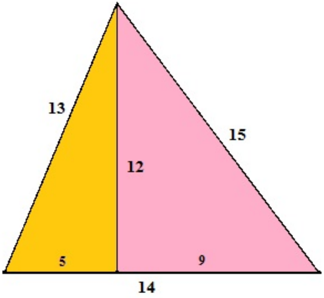
Consequently,

$$\left| \frac{1}{z^{n+1}} Q_n(-z) \right| \geq \frac{1}{|z(1-z)|^{n+1}} - \sum_{j=0}^{\infty} \binom{2n+1+j}{n} |z|^j.$$

Now estimate the sum on the right.

Part II

Diophantine equations related to triangles



Joint work with

John B. Cosgrave

Dublin, Ireland

1. Heronian Triangles

Heronian triangle:

A triangle whose side lengths and area are all integers.

1. Heronian Triangles

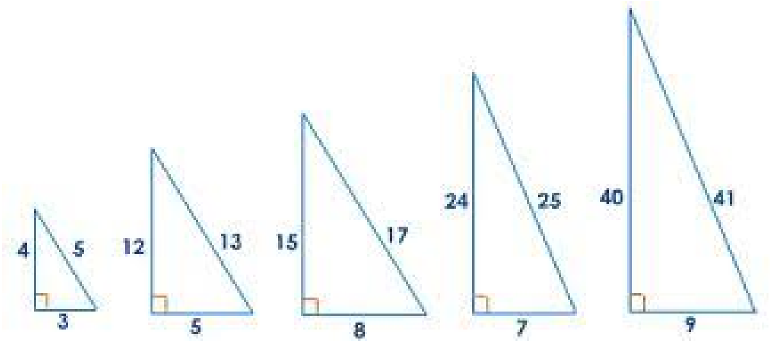
Heronian triangle:
A triangle whose side lengths and area are all integers.

Do they exist?

1. Heronian Triangles

Heronian triangle:
A triangle whose side lengths and area are all integers.

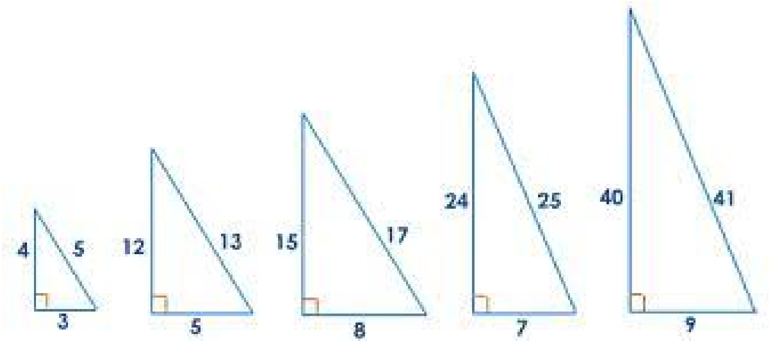
Do they exist? Consider



1. Heronian Triangles

Heronian triangle:
A triangle whose side lengths and area are all integers.

Do they exist? Consider



All Pythagorean triangles are Heronian.

Heronian triangles are named after

Hero or **Heron of Alexandria**, c. 10 AD – c. 70 AD.

Heronian triangles are named after

Hero or **Heron of Alexandria**, c. 10 AD – c. 70 AD.

(17th-century German depiction)

A mathematician and engineer, active in his native city of Alexandria, Roman Egypt.

A mathematician and engineer, active in his native city of Alexandria, Roman Egypt.

Considered the greatest experimenter of antiquity.

A mathematician and engineer, active in his native city of Alexandria, Roman Egypt.

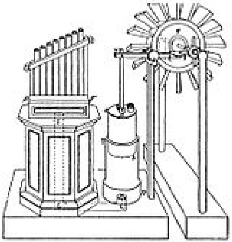
Considered the greatest experimenter of antiquity.

His work is representative of the Hellenistic scientific tradition. (Wikipedia)

A mathematician and engineer, active in his native city of Alexandria, Roman Egypt.

Considered the greatest experimenter of antiquity.

His work is representative of the Hellenistic scientific tradition. (Wikipedia)



Hero’s mathematical contributions:

Hero's mathematical contributions:

• A method for iteratively computing the square root of a number.

Hero's mathematical contributions:

• A method for iteratively computing the square root of a number.

• The **Heronian mean**: For $A, B \geq 0$,

$$H = \frac{1}{3}(A + \sqrt{AB} + B)$$

Hero's mathematical contributions:

- A method for iteratively computing the square root of a number.

- The **Heronian mean**: For $A, B \geq 0$,

$$H = \frac{1}{3}(A + \sqrt{AB} + B) = \frac{2}{3} \cdot \frac{A+B}{2} + \frac{1}{3} \cdot \sqrt{AB}.$$

Hero's mathematical contributions:

• A method for iteratively computing the square root of a number.

• The **Heronian mean**: For $A, B \geq 0$,

$$H = \frac{1}{3}(A + \sqrt{AB} + B) = \frac{2}{3} \cdot \frac{A+B}{2} + \frac{1}{3} \cdot \sqrt{AB}.$$

• A formula for finding the area of a triangle from its side lengths: Given a triangle with side lengths a, b, c, the area is

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \quad \text{where} \quad s = \frac{a+b+c}{2}.$$

Hero's mathematical contributions:

• A method for iteratively computing the square root of a number.

• The **Heronian mean**: For $A, B \geq 0$,

$$H = \frac{1}{3}(A + \sqrt{AB} + B) = \frac{2}{3} \cdot \frac{A+B}{2} + \frac{1}{3} \cdot \sqrt{AB}.$$

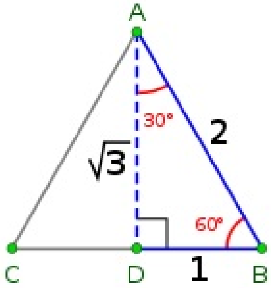
• A formula for finding the area of a triangle from its side lengths: Given a triangle with side lengths a, b, c, the area is

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \quad \text{where} \quad s = \frac{a+b+c}{2}.$$

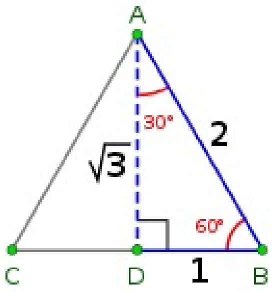
Back to Heronian triangles:

Can an **equilateral** triangle be Heronian?

Can an **equilateral** triangle be Heronian?

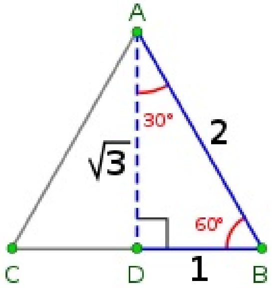


Can an **equilateral** triangle be Heronian?



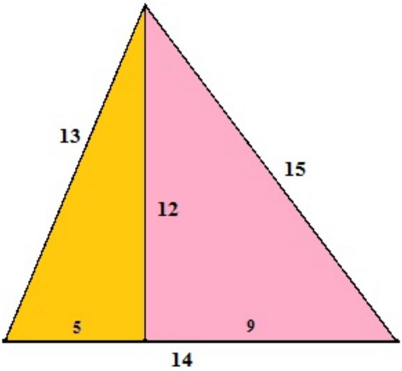
Obviously not.

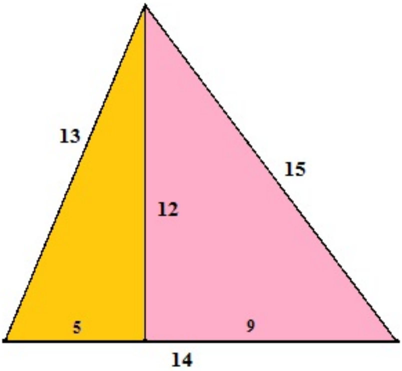
Can an **equilateral** triangle be Heronian?



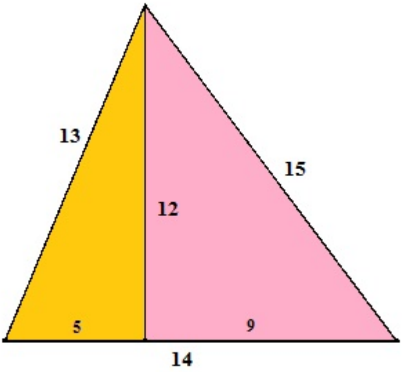
Obviously not.

Then, how about “near equilateral"?


13
15
12
5
9
14



The 2nd-smallest example of a Heronian triangle of side lenghts $(n-1, n, n+1)$, after $(3, 4, 5)$.



The 2nd-smallest example of a Heronian triangle of side lenghts $(n-1, n, n+1)$, after $(3, 4, 5)$.

Are there more Heronian triangles of this type?

The condition for a triangle of side lenghts $(n-1, n, n+1)$ to be Heronian leads to the Pell equation

$$n^2 - 12y^2 = 4,$$

The condition for a triangle of side lenghts $(n-1, n, n+1)$ to be Heronian leads to the Pell equation

$$n^2 - 12y^2 = 4, \quad \text{or} \quad x^2 - 3y^2 = 1.$$

The condition for a triangle of side lenghts $(n-1, n, n+1)$ to be Heronian leads to the Pell equation

$$n^2 - 12y^2 = 4, \quad \text{or} \quad x^2 - 3y^2 = 1.$$

Solving these: We get $n = n_j$ with $n_0 = 2, n_1 = 4$, and

$$n_j = 4n_{j-1} - n_{j-2} \qquad (j \geq 2),$$

The condition for a triangle of side lenghts $(n-1, n, n+1)$ to be Heronian leads to the Pell equation

$$n^2 - 12y^2 = 4, \quad \text{or} \quad x^2 - 3y^2 = 1.$$

Solving these: We get $n = n_j$ with $n_0 = 2, n_1 = 4$, and

$$n_j = 4n_{j-1} - n_{j-2} \qquad (j \geq 2),$$

and the explicit expansion

$$n_j = \left(2 + \sqrt{3}\right)^j + \left(2 - \sqrt{3}\right)^j.$$

The condition for a triangle of side lenghts $(n-1, n, n+1)$ to be Heronian leads to the Pell equation

$$n^2 - 12y^2 = 4, \quad \text{or} \quad x^2 - 3y^2 = 1.$$

Solving these: We get $n = n_j$ with $n_0 = 2, n_1 = 4$, and

$$n_j = 4n_{j-1} - n_{j-2} \qquad (j \geq 2),$$

and the explicit expansion

$$n_j = \left(2+\sqrt{3}\right)^j + \left(2-\sqrt{3}\right)^j.$$

This goes back to Edward Sang (1864) and R. Hoppe (1880).

Rediscovered later, for instance by L. Aubry (1911).

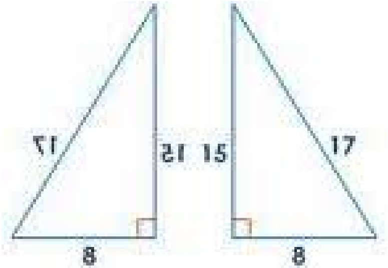
Can there be Heronian triangles that are even closer to being equilateral, namely with side lengths $(n, n, n-1)$?

Can there be Heronian triangles that are even closer to being equilateral, namely with side lengths $(n, n, n-1)$?

Again, the answer is Yes:

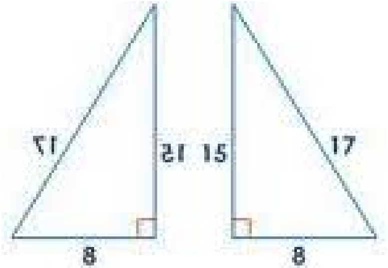
Can there be Heronian triangles that are even closer to being equilateral, namely with side lengths $(n, n, n-1)$?

Again, the answer is Yes: Combine these two:



Can there be Heronian triangles that are even closer to being equilateral, namely with side lengths $(n, n, n-1)$?

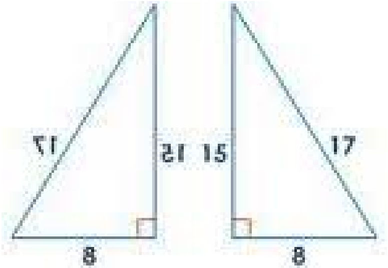
Again, the answer is Yes: Combine these two:



In this case we get the sequence 1, 17, 241, 3361, 46817, . . .,

Can there be Heronian triangles that are even closer to being equilateral, namely with side lengths $(n, n, n-1)$?

Again, the answer is Yes: Combine these two:



In this case we get the sequence 1, 17, 241, 3361, 46817, ..., satisfying the 3-rd order recurrence

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

2. Multiplicative Orders of Factorials

Surprisingly, the two “Heronian sequences" occur in an entirely different setting.

2. Multiplicative Orders of Factorials

Surprisingly, the two “Heronian sequences" occur in an entirely different setting.

We begin with *Wilson’s Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

2. Multiplicative Orders of Factorials

Surprisingly, the two “Heronian sequences" occur in an entirely different setting.

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot\ldots\cdot\tfrac{p-1}{2}\,\tfrac{p+1}{2}\cdot\ldots\cdot(p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

2. Multiplicative Orders of Factorials

Surprisingly, the two “Heronian sequences" occur in an entirely different setting.

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot \ldots \cdot \tfrac{p-1}{2}\,\tfrac{p+1}{2}\cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

Thus, with Wilson's Theorem,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

2. Multiplicative Orders of Factorials

Surprisingly, the two “Heronian sequences" occur in an entirely different setting.

We begin with *Wilson’s Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

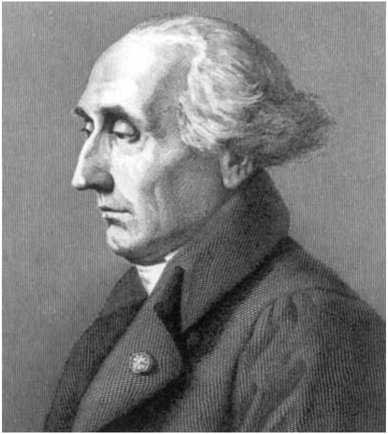
Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot\ldots\cdot\tfrac{p-1}{2}\tfrac{p+1}{2}\cdot\ldots\cdot(p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

Thus, with Wilson’s Theorem,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

This was apparently first observed by Lagrange (1773).



John Wilson
1741–1793

Joseph-Louis Lagrange
1736–1813

This congruence,

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod{4}$ the RHS is -1, so

$$\operatorname{ord}_p\left(\left(\frac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod{4}.$$

This congruence,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod{4}$ the RHS is -1, so

$$\mathrm{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod{4}.$$

In the case $p \equiv 3 \pmod{4}$ we get

$$\left(\tfrac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

This congruence,

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod 4$ the RHS is -1, so

$$\mathrm{ord}_p\left(\left(\frac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod 4.$$

In the case $p \equiv 3 \pmod 4$ we get

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

What is the sign on the right?

Theorem (Mordell, 1961)

For a prime $p \equiv 3 \pmod 4$,

$$\left(\frac{p-1}{2}\right)! \equiv -1 \pmod p \quad \Leftrightarrow \quad h(-p) \equiv 1 \pmod 4,$$

where $h(-p)$ *is the class number of* $\mathbb{Q}(\sqrt{-p})$.

Theorem (Mordell, 1961)

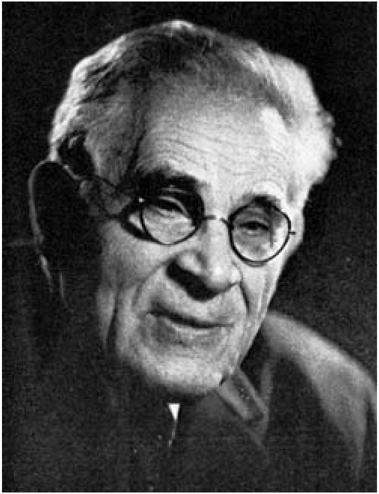
For a prime $p \equiv 3 \pmod 4$,

$$\left(\tfrac{p-1}{2}\right)! \equiv -1 \pmod p \quad \Leftrightarrow \quad h(-p) \equiv 1 \pmod 4,$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$.

First mentioned in a book by Venkov (1937, in Russian). Discovered independently by Chowla.

This completely determines the order mod p of $\left(\frac{p-1}{2}\right)!$.



Louis J. Mordell
1888–1972

Sarvadaman Chowla
1907–1995

More generally, what can we say about the orders (mod p) of

$$\left(\frac{p-1}{M}\right)!, \qquad (p \equiv 1 \pmod{M})$$

for $M \geq 3$?

More generally, what can we say about the orders (mod p) of

$$\left(\frac{p-1}{M}\right)!, \qquad (p \equiv 1 \pmod{M})$$

for $M \geq 3$?

In general, the orders are unbounded.

More generally, what can we say about the orders (mod p) of

$$\left(\frac{p-1}{M}\right)!, \qquad (p \equiv 1 \pmod{M})$$

for $M \geq 3$?

In general, the orders are unbounded.

Of particular interest are the cases $M = 3, 4$ and 6.

More generally, what can we say about the orders (mod p) of

$$\left(\frac{p-1}{M}\right)!, \qquad (p \equiv 1 \pmod{M})$$

for $M \geq 3$?

In general, the orders are unbounded.

Of particular interest are the cases $M = 3, 4$ and 6.

Reason is the existence of some deep binomial coefficient congruences.

More generally, what can we say about the orders (mod p) of

$$\left(\frac{p-1}{M}\right)!, \qquad (p \equiv 1 \pmod{M})$$

for $M \geq 3$?

In general, the orders are unbounded.

Of particular interest are the cases $M = 3, 4$ and 6.

Reason is the existence of some deep binomial coefficient congruences.

Here: We'll consider the case $M = 4$.

In 1828, Gauss proved the following remarkable congruence.

Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$.
(a is then uniquely determined).

In 1828, Gauss proved the following remarkable congruence.

Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$. (a is then uniquely determined).

Theorem (Gauss, 1828)

Let p and a be as above. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

In 1828, Gauss proved the following remarkable congruence.

Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$. (a is then uniquely determined).

Theorem (Gauss, 1828)

Let p and a be as above. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

There are similar congruences for $\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}}$ (Jacobi, 1837), and others.

C. F. Gauss
1777–1855

C. G. J. Jacobi
1804–1851

Let's look at the first 30 primes $p \equiv 1 \pmod 4$:

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	1	97	20	32	197	92	98
13	6	12	101	46	100	229	168	38
17	7	16	109	7	27	233	36	116
29	23	7	113	32	28	241	130	16
37	21	18	137	90	136	257	120	32
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	193	89	64	313	109	312

Let's look at the first 30 primes $p \equiv 1 \pmod 4$:

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	1	97	20	32	197	92	98
13	6	12	101	46	100	229	168	38
17	7	16	109	7	27	233	36	116
29	23	7	113	32	28	241	130	16
37	21	18	137	90	136	257	120	32
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	193	89	64	313	109	312

- Orders seem to be unbounded.

Let's look at the first 30 primes $p \equiv 1 \pmod 4$:

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	1	97	20	32	197	92	98
13	6	12	101	46	100	229	168	38
17	7	16	109	7	27	233	36	116
29	23	7	113	32	28	241	130	16
37	21	18	137	90	136	257	120	32
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	193	89	64	313	109	312

- Orders seem to be unbounded.
- Some $\frac{p-1}{4}!$ are primitive roots.

Let's look at the first 30 primes $p \equiv 1 \pmod 4$:

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	1	97	20	32	197	92	98
13	6	12	101	46	100	229	168	38
17	7	16	109	7	27	233	36	116
29	23	7	113	32	28	241	130	16
37	21	18	137	90	136	257	120	32
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	193	89	64	313	109	312

- Orders seem to be unbounded.
- Some $\frac{p-1}{4}!$ are primitive roots.
- Of particular interest: Orders that are powers of 2.

Let's look at the first 30 primes $p \equiv 1 \pmod 4$:

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	**1**	**97**	20	**32**	197	92	98
13	6	12	101	46	100	229	168	38
17	7	**16**	109	7	27	233	36	116
29	23	7	113	32	28	**241**	130	**16**
37	21	18	137	90	136	**257**	120	**32**
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	**193**	89	**64**	313	109	312

- Orders seem to be unbounded.
- Some $\frac{p-1}{4}!$ are primitive roots.
- Of particular interest: Orders that are powers of 2.

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *if and only if* $p = p_k$, *a prime element of the sequence defined by*

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *if and only if* $p = p_k$, *a prime element of the sequence defined by* $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, *and*

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *if and only if* $p = p_k$, *a prime element of the sequence defined by* $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, *and*

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

The proof relies on Gauss's binomial coefficient theorem.

Theorem

Let $p \equiv 1 \pmod 4$ *be a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *if and only if* $p = p_k$, *a prime element of the sequence defined by* $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, *and*

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

The proof relies on Gauss's binomial coefficient theorem.

Recall: The sequence p_k is the second “Heronian" sequence.

Related to this we introduce the following terminology.

Definition

Let $p \equiv 1 \pmod 4$ be a prime. If

$$\mathrm{ord}_p\left(\tfrac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ell \geq 0,$$

we say that p is a Gauss prime of level ℓ.

Related to this we introduce the following terminology.

Definition

Let $p \equiv 1 \pmod 4$ be a prime. If

$$\operatorname{ord}_p\left(\tfrac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ell \geq 0,$$

we say that p is a Gauss prime of level ℓ.

By the Theorem:

- $p = 5$ is the only Gauss prime of level 0.

Related to this we introduce the following terminology.

Definition

Let $p \equiv 1 \pmod{4}$ be a prime. If

$$\mathrm{ord}_p\left(\tfrac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ell \geq 0,$$

we say that p is a Gauss prime of level ℓ.

By the Theorem:

- $p = 5$ is the only Gauss prime of level 0.
- There are no Gauss primes of levels 1, 2, or 3.

Related to this we introduce the following terminology.

Definition

Let $p \equiv 1 \pmod 4$ be a prime. If

$$\mathrm{ord}_p\left(\tfrac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ell \geq 0,$$

we say that p is a Gauss prime of level ℓ.

By the Theorem:
- $p = 5$ is the only Gauss prime of level 0.
- There are no Gauss primes of levels 1, 2, or 3.

By the Definition:
- Any Fermat prime F_n is a Gauss prime of level $n + 2$.

Related to this we introduce the following terminology.

Definition

Let $p \equiv 1 \pmod 4$ be a prime. If

$$\operatorname{ord}_p\left(\frac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ell \geq 0,$$

we say that p is a Gauss prime of level ℓ.

By the Theorem:

- $p = 5$ is the only Gauss prime of level 0.
- There are no Gauss primes of levels 1, 2, or 3.

By the Definition:

- Any Fermat prime F_n is a Gauss prime of level $n + 2$.
- For instance, $F_2 = 17$ is indeed a Gauss prime of level 4.

All Gauss primes $p < 10^{14}$ ($p < 10^{16}$ for $\ell = 5$) and $\ell \leq 20$.

ℓ	primes
0	5 only
1–3	none
4	**17, 241, 3361, 46817, 652081,** ...
5	97, 257, 929, 262337, 200578817
6	193, 65537
7	641, 12055618177
8	3200257
9	93418448897
10	285697, 345089, 11118593
11	120833, 1249520060417
12	12289
13	1908737, 10812547073
14	114689, 8780414977
15	
16	1179649, 27590657, 2742091777
17	
18	786433, 3225052512257

Recall: Theorem says that $p \equiv 1 \pmod 4$ is a level-4 Gauss prime iff $p = p_k$ is a prime element of the sequence defined by $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, and

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

Recall: Theorem says that $p \equiv 1 \pmod{4}$ is a level-4 Gauss prime iff $p = p_k$ is a prime element of the sequence defined by $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, and

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

When are these elements prime?

Recall: Theorem says that $p \equiv 1 \pmod 4$ is a level-4 Gauss prime iff $p = p_k$ is a prime element of the sequence defined by $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, and

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

When are these elements prime?

k	p_k	prime
1	17	yes
2	241	yes
3	3 361	yes
4	46 817	yes
5	652 081	yes
6	9 082 321	no

Recall: Theorem says that $p \equiv 1 \pmod 4$ is a level-4 Gauss prime iff $p = p_k$ is a prime element of the sequence defined by $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, and

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

When are these elements prime?

k	p_k	prime
1	17	yes
2	241	yes
3	3 361	yes
4	46 817	yes
5	652 081	yes
6	9 082 321	no

Surprisingly, the next prime in this sequence is p_{131}, then p_{200}.

Recall: Theorem says that $p \equiv 1 \pmod 4$ is a level-4 Gauss prime iff $p = p_k$ is a prime element of the sequence defined by $p_0 = 1$, $p_1 = 17$, $p_2 = 241$, and

$$p_k = 15p_{k-1} - 15p_{k-2} + p_{k-3} \qquad (k \geq 3).$$

When are these elements prime?

k	p_k	prime
1	17	yes
2	241	yes
3	3 361	yes
4	46 817	yes
5	652 081	yes
6	9 082 321	no

Surprisingly, the next prime in this sequence is p_{131}, then p_{200}. We'll return to this later.

3. Gauss Factorials

We define the **Gauss factorial** by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

3. Gauss Factorials

We define the **Gauss factorial** by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

Analogue of Wilson's theorem for composite moduli:

Theorem (Gauss)

For any integer $n \geq 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod{n} & \text{otherwise}, \end{cases}$$

where p is an odd prime and α is a positive integer.

3. Gauss Factorials

We define the **Gauss factorial** by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

Analogue of Wilson's theorem for composite moduli:

Theorem (Gauss)

For any integer $n \ge 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod{n} & \text{otherwise}, \end{cases}$$

where p is an odd prime and α is a positive integer.

The first case indicates exactly those n that have primitive roots.

Many questions can be extended to composite moduli.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

• Obviously, this holds for $n = 5$.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

- Obviously, this holds for $n = 5$.
- Next: $n = 205, 725, 1025, 1105, \ldots$

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

- Obviously, this holds for $n = 5$.
- Next: $n = 205$, 725, 1025, 1105, $\ldots$
- A total of 37 109 solutions up to 10^6.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

- Obviously, this holds for $n = 5$.
- Next: $n = 205, 725, 1025, 1105, \ldots$
- A total of 37 109 solutions up to 10^6.
- All of these (except $n = 5$) have at least two distinct prime factors $\equiv 1 \pmod 4$.

Many questions can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur.

We obtained numerous other results on $(\frac{n-1}{M})_n!$ modulo n for general $M \geq 3$, and in particular for $M = 3, 4$ and 6.

Here: One specific question: For which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

- Obviously, this holds for $n = 5$.
- Next: $n = 205$, 725, 1025, 1105, ...
- A total of 37 109 solutions up to 10^6.
- All of these (except $n = 5$) have at least two distinct prime factors $\equiv 1 \pmod 4$.
- Is this true in general?

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

Surprisingly, there **are** other solutions with **only one** prime factor $\equiv 1 \pmod 4$.

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

Surprisingly, there **are** other solutions with **only one** prime factor $\equiv 1 \pmod 4$. The three smallest ones are:

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

Surprisingly, there **are** other solutions with **only one** prime factor $\equiv 1 \pmod 4$. The three smallest ones are:

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

Recall: 46817 and 652081 are in our “Heronian" sequence.

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod{n}?$$

Surprisingly, there **are** other solutions with **only one** prime factor $\equiv 1 \pmod 4$. The three smallest ones are:

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

Recall: 46817 and 652081 are in our “Heronian" sequence.

The next smallest solution known to us has 155 digits, with p_{133} (mentioned above) being its only prime factor $\equiv 1 \pmod 4$.

Again, for which integers $n \equiv 1 \pmod 4$ do we have

$$\left(\tfrac{n-1}{4}\right)_n! \equiv 1 \pmod n?$$

Surprisingly, there **are** other solutions with **only one** prime factor $\equiv 1 \pmod 4$. The three smallest ones are:

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

Recall: 46817 and 652081 are in our “Heronian" sequence.

The next smallest solution known to us has 155 digits, with p_{133} (mentioned above) being its only prime factor $\equiv 1 \pmod 4$.

All this can be fully explained.

4. Factors of p_k

All $k \leq 10^5$ for which p_k is a prime or a *probable prime*:

1	200	5 598	12 483
2	296	6 683	*13 536*
3	350	7 445	*18 006*
4	519	8 775	*18 995*
5	704	8 786	*48 773*
131	950	11 565	*93 344*

All $k \leq 10^5$ for which p_k is a prime or a *probable prime*:

1	200	5 598	12 483
2	296	6 683	*13 536*
3	350	7 445	*18 006*
4	519	8 775	*18 995*
5	704	8 786	*48 773*
131	950	11 565	*93 344*

Are there necessary conditions for p_k to be a prime?

This would speed up computations.

Using standard methods from theory of linear recurrences:

$$p_k = a_{k+1}^2 + a_k^2 \qquad (k \geq 0),$$

where the sequence $\{a_k\}$ satisfies $a_0 = 0, a_1 = 1$, and

$$a_k = 4a_{k-1} - a_{k-2} \qquad (k \geq 2).$$

Using standard methods from theory of linear recurrences:

$$p_k = a_{k+1}^2 + a_k^2 \qquad (k \geq 0),$$

where the sequence $\{a_k\}$ satisfies $a_0 = 0, a_1 = 1$, and

$$a_k = 4a_{k-1} - a_{k-2} \qquad (k \geq 2).$$

In fact, $a_k = U_k(4, 1)$, an instance of a generalized Lucas sequence. Known from the general case:

$$a_k = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right) \qquad (k \geq 0).$$

Using standard methods from theory of linear recurrences:

$$p_k = a_{k+1}^2 + a_k^2 \qquad (k \geq 0),$$

where the sequence $\{a_k\}$ satisfies $a_0 = 0, a_1 = 1$, and

$$a_k = 4a_{k-1} - a_{k-2} \qquad (k \geq 2).$$

In fact, $a_k = U_k(4,1)$, an instance of a generalized Lucas sequence. Known from the general case:

$$a_k = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right) \qquad (k \geq 0).$$

To simplify notation, we set

$$\alpha := 2+\sqrt{3}, \qquad m := 2k+1,$$

Using standard methods from theory of linear recurrences:

$$p_k = a_{k+1}^2 + a_k^2 \qquad (k \geq 0),$$

where the sequence $\{a_k\}$ satisfies $a_0 = 0, a_1 = 1$, and

$$a_k = 4a_{k-1} - a_{k-2} \qquad (k \geq 2).$$

In fact, $a_k = U_k(4,1)$, an instance of a generalized Lucas sequence. Known from the general case:

$$a_k = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right) \qquad (k \geq 0).$$

To simplify notation, we set

$$\alpha := 2+\sqrt{3}, \qquad m := 2k+1,$$

Then α is a unit in $\mathbb{Q}[\sqrt{3}]$; in particular, $2-\sqrt{3} = \alpha^{-1}$.

Combining everything:

$$p_k = \frac{1}{3\alpha^m}\left(\alpha^{2m} - \alpha^m + 1\right).$$

Combining everything:

$$p_k = \frac{1}{3\alpha^m}\left(\alpha^{2m} - \alpha^m + 1\right).$$

This indicates: Divisibility of cyclotomic polynomials in α will be involved.

Combining everything:

$$p_k = \frac{1}{3\alpha^m}\left(\alpha^{2m} - \alpha^m + 1\right).$$

This indicates: Divisibility of cyclotomic polynomials in α will be involved. An immediate factorization gives

$$p_k = \frac{1}{3\alpha^m}\frac{(\alpha^{6m}-1)(\alpha^m-1)}{(\alpha^{3m}-1)(\alpha^{2m}-1)}.$$

Combining everything:

$$p_k = \frac{1}{3\alpha^m}\left(\alpha^{2m} - \alpha^m + 1\right).$$

This indicates: Divisibility of cyclotomic polynomials in α will be involved. An immediate factorization gives

$$p_k = \frac{1}{3\alpha^m}\frac{(\alpha^{6m}-1)(\alpha^m-1)}{(\alpha^{3m}-1)(\alpha^{2m}-1)}.$$

We also need the well-known factorization

$$x^n - 1 = \prod_{d|n}\Phi_d(x).$$

Combining everything:

$$p_k = \frac{1}{3\alpha^m}\left(\alpha^{2m} - \alpha^m + 1\right).$$

This indicates: Divisibility of cyclotomic polynomials in α will be involved. An immediate factorization gives

$$p_k = \frac{1}{3\alpha^m}\frac{(\alpha^{6m}-1)(\alpha^m-1)}{(\alpha^{3m}-1)(\alpha^{2m}-1)}.$$

We also need the well-known factorization

$$x^n - 1 = \prod_{d|n}\Phi_d(x).$$

and the following lemma: If $n \geq 3$ and $\alpha = 2+\sqrt{3}$, then

$$\frac{1}{\alpha^{\frac{1}{2}\varphi(n)}}\Phi_n(\alpha) \in \mathbb{Z},$$

where $\varphi(n)$ is the Euler totient function.

Using this and further technical lemmas, we get

Theorem

Let $k \geq 0$ and suppose that $\gamma \geq 0$ is such that $3^\gamma \mid\mid 2k+1$. Then $p_n \mid p_k$ whenever $2n+1 \mid 2k+1$ and $3^\gamma \mid 2n+1$.

Using this and further technical lemmas, we get

Theorem

Let $k \geq 0$ and suppose that $\gamma \geq 0$ is such that $3^{\gamma} \parallel 2k+1$. Then $p_n \mid p_k$ whenever $2n+1 \mid 2k+1$ and $3^{\gamma} \mid 2n+1$.

An immediate consequence:

Corollary

If p_k is a prime, then $2k+1$ is a prime or a power of 3.

Using this and further technical lemmas, we get

Theorem

Let $k \geq 0$ and suppose that $\gamma \geq 0$ is such that $3^\gamma \parallel 2k+1$. Then $p_n \mid p_k$ whenever $2n+1 \mid 2k+1$ and $3^\gamma \mid 2n+1$.

An immediate consequence:

Corollary

If p_k is a prime, then $2k+1$ is a prime or a power of 3.

Example:

k	$2k+1$	k	$2k+1$
1	3	5	11
2	5	131	263
3	7	200	401
4	9	296	593

5. Back to Heronian Triangles

Recall:

$$a_k = U_k(4,1) = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right).$$

5. Back to Heronian Triangles

Recall:

$$a_k = U_k(4,1) = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right).$$

It turns out: The sequence $\{n_k\}$ that gives Heronian triangles with sides $(n_k - 1, n_k, n_k + 1)$ is the companion sequence

$$n_k = V_k(4,1) = \left(2+\sqrt{3}\right)^k + \left(2-\sqrt{3}\right)^k.$$

5. Back to Heronian Triangles

Recall:

$$a_k = U_k(4,1) = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right).$$

It turns out: The sequence $\{n_k\}$ that gives Heronian triangles with sides $(n_k - 1, n_k, n_k + 1)$ is the companion sequence

$$n_k = V_k(4,1) = \left(2+\sqrt{3}\right)^k + \left(2-\sqrt{3}\right)^k.$$

It follows from the theory that

$$n_k = a_{k+1} - a_{k-1} \qquad (k \geq 1).$$

Thank you

"You know, most people's favourite number is 7, but mine is 6273990103648829910048253048103855722295710049274010154829477388859173 89."