About the divisors of $a^n + 1$ and their interesting connection to prime numbers

Matthias Heinlein

05.09.2013

Workshop "'Probability, Analysis and Geometry"

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$.

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$. If $gcd(a, b) = 1$, a and b are coprime/relatively prime.

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$. If $gcd(a, b) = 1$, a and b are coprime/relatively prime.
- Congruences:

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$. If $gcd(a, b) = 1$, a and b are coprime/relatively prime.
- Congruences:$a \equiv b \pmod{c}$ denotes that $c \mid a - b$, read as "a is congruent to b modulo c",

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$. If $gcd(a, b) = 1$, a and b are coprime/relatively prime.
- Congruences:$a \equiv b \pmod{c}$ denotes that $c \mid a - b$, read as "a is congruent to b modulo c", e.g. $17 \equiv 7 \pmod{5}$, since $5 \mid 10 = 17 - 7$.

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\gcd(a, b) \geq 1$. If $gcd(a, b) = 1$, a and b are coprime/relatively prime.
- Congruences:$a \equiv b \pmod{c}$ denotes that $c \mid a - b$, read as "a is congruent to b modulo c", e.g. $17 \equiv 7 \pmod{5}$, since $5 \mid 10 = 17 - 7$.
- If $\gcd(a, c) = 1$, define $\mathrm{ord}_c(a) := \min\{n \mid a^n \equiv 1 \pmod{c}\}$.

Number theoretical basics

Convention

All numbers in this talk are natural numbers (1,2,3,4,...).

Basics

- $a \mid b$ denotes that a is a divisor of b.
- $\gcd(a,b)$ denotes the greatest common divisor of a and b, $\gcd(a,b) \geq 1$. If $gcd(a,b) = 1$, a and b are coprime/relatively prime.
- Congruences:$a \equiv b \pmod{c}$ denotes that $c \mid a - b$, read as "a is congruent to b modulo c", e.g. $17 \equiv 7 \pmod{5}$, since $5 \mid 10 = 17 - 7$.
- If $\gcd(a,c) = 1$, define $\mathrm{ord}_c(a) := \min\{n \mid a^n \equiv 1 \pmod{c}\}$. e.g. $\mathrm{ord}_7(2) = 3$, since $2^1 = 2 \not\equiv 1, 2^2 = 4 \not\equiv 1, 2^3 = 8 \equiv 1 \pmod{7}$.

P_a-numbers

P_a-numbers

Definition

P_a-numbers

Definition

For fixed number $a \geq 2$

$$a^n + 1$$

P_a-numbers

Definition

For fixed number $a \geq 2$

$$d \mid a^n + 1$$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\}$$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \; \exists\, n : d \mid a^n + 1\} = \{d \mid \; \exists\, n : a^n \equiv -1 \pmod{d}\}$$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \ \exists\, n : d \mid a^n + 1\} = \{d \mid \ \exists\, n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \ \exists\, n : d \mid a^n + 1\} = \{d \mid \ \exists\, n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1,$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, 2$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists\, n : d \mid a^n + 1\} = \{d \mid \exists\, n : a^n \equiv -1 \pmod d\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2},$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod d\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2}, 3,$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2}, 3, 5,$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists\, n : d \mid a^n + 1\} = \{d \mid \exists\, n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2}, 3, 5, 7$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2}, 3, 5, \cancel{7}$

P_a-numbers

Definition

For fixed number $a \geq 2$ we define

$$P_a := \{d \mid \exists n : d \mid a^n + 1\} = \{d \mid \exists n : a^n \equiv -1 \pmod{d}\}$$

If $d \in P_a$, then d is called "good for a", otherwise "bad".

Example $a = 2$, what are the divisors of $2^n + 1$?

$P_2 = \{1, \cancel{2}, 3, 5, \cancel{7}, 9, 11, 13, 17, 19, 25, 27, 29, 33, ...\}$

Criterias

Criterias

Task

For given a and d, we want to check if d is good for a ($d \in P_a$).

Criterias

Task

For given a and d, we want to check if d is good for a ($d \in P_a$).

Some criterias

Criterias

Task

For given a and d, we want to check if d is good for a ($d \in P_a$).

Some criterias

- Divisors of good numbers are good. Multiples of bad numbers are bad.

Criterias

Task

For given a and d, we want to check if d is good for a ($d \in P_a$).

Some criterias

- Divisors of good numbers are good. Multiples of bad numbers are bad.
- If d is an odd prime:

Criterias

Task

For given a and d, we want to check if d is good for a ($d \in P_a$).

Some criterias

- Divisors of good numbers are good. Multiples of bad numbers are bad.
- If d is an odd prime: d is good $\Leftrightarrow$ $\mathrm{ord}_d(a)$ is even.

Product of good numbers

Product of good numbers

Example

$3, 5, 11 \in P_2$.

Product of good numbers

Example

$3, 5, 11 \in P_2$.
$3 \cdot 11 = 33 \in P_2$.

Product of good numbers

Example

$3, 5, 11 \in P_2$.
$3 \cdot 11 = 33 \in P_2$.
$3 \cdot 5 = 15 \notin P_2$.

Product of good numbers

Example

$3, 5, 11 \in P_2$.
$3 \cdot 11 = 33 \in P_2$.
$3 \cdot 5 = 15 \notin P_2$.

Theorem

Product of good numbers

Example

$3, 5, 11 \in P_2$.
$3 \cdot 11 = 33 \in P_2$.
$3 \cdot 5 = 15 \notin P_2$.

Theorem

The product of two good numbers d and e is good again

Product of good numbers

Example

$3, 5, 11 \in P_2$.
$3 \cdot 11 = 33 \in P_2$.
$3 \cdot 5 = 15 \notin P_2$.

Theorem

The product of two good numbers d and e is good again if and only if $\mathrm{ord}_d(a)$ and $\mathrm{ord}_e(a)$ contain the same power of 2.

Product of good numbers

Example

$3, 5, 11 \in P_2$. $\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_{11}(2) = 10$, both contain 2^1

$3 \cdot 11 = 33 \in P_2$.

$3 \cdot 5 = 15 \notin P_2$.

Theorem

The product of two good numbers d and e is good again if and only if $\mathrm{ord}_d(a)$ and $\mathrm{ord}_e(a)$ contain the same power of 2.

Product of good numbers

Example

$3, 5, 11 \in P_2$. $\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_{11}(2) = 10$, both contain 2^1

$3 \cdot 11 = 33 \in P_2$. $\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_5(2) = 4$, contain different powers of 2.

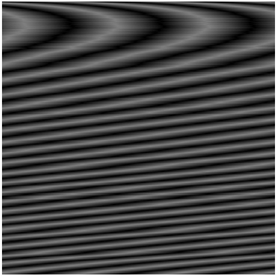
$3 \cdot 5 = 15 \notin P_2$.

Theorem

The product of two good numbers d and e is good again if and only if $\mathrm{ord}_d(a)$ and $\mathrm{ord}_e(a)$ contain the same power of 2.

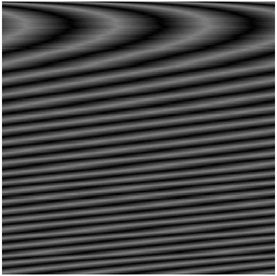
Woodstone-Visualization

Woodstone-Visualization

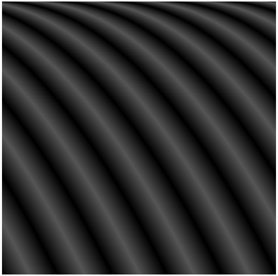


Prime numbers

Woodstone-Visualization

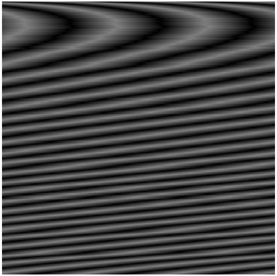


Prime numbers

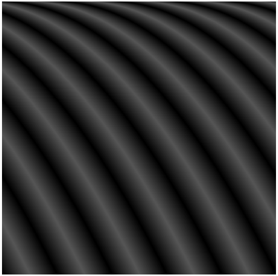


Square numbers

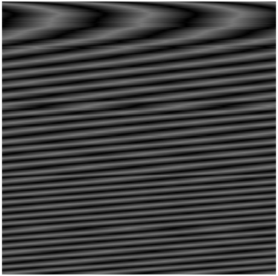
Woodstone-Visualization



Prime numbers



Square numbers



P_2-numbers

Connection with prime numbers

Large gaps in prime numbers

Gaps in prime numbers

2 3 5 7 11 13 17 19 23 29

Large gaps in prime numbers

Gaps in prime numbers

2		3		5		7		11		13		17		19		23		29
	1		2		2		4		2		4		2		4		6	

Large gaps in prime numbers

Gaps in prime numbers

2		3		5		7		11		13		17		19		23		29
	1		2		2		4		2		4		2		4		6	

Theorem

One can find abitrarily large gaps between consecutive primes.

Large gaps in prime numbers

Gaps in prime numbers

2		3		5		7		11		13		17		19		23		29
	1		2		2		4		2		4		2		4		6	

Theorem

One can find abitrarily large gaps between consecutive primes.

Proof.

To find a gap of length $\geq n$, define $a := (n+1)!$, so

Large gaps in prime numbers

Gaps in prime numbers

2		3		5		7		11		13		17		19		23		29
	1		2		2		4		2		4		2		4		6	

Theorem

One can find abitrarily large gaps between consecutive primes.

Proof.

To find a gap of length $\geq n$, define $a := (n+1)!$, so

$$\begin{aligned} 2 \mid a+2 &\Rightarrow \text{ no prime number} \\ 3 \mid a+3 &\Rightarrow \text{ no prime number} \\ &\dots \\ (n+1) \mid a+(n+1) &\Rightarrow \text{ no prime number} \end{aligned}$$

Large gaps in P_a-numbers

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Gaps in P_a

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Gaps in P_a

To find gaps of length n, find a number x which satisfies the conditions:

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Gaps in P_a

To find gaps of length n, find a number x which satisfies the conditions:

$$\begin{aligned} x+1 &\equiv 0 \pmod{q_1} \\ x+2 &\equiv 0 \pmod{q_2} \\ &\ldots \\ x+n &\equiv 0 \pmod{q_n} \end{aligned}$$

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Gaps in P_a

To find gaps of length n, find a number x which satisfies the conditions:

$$\begin{aligned} x+1 &\equiv 0 \pmod{q_1} \\ x+2 &\equiv 0 \pmod{q_2} \\ &\ldots \\ x+n &\equiv 0 \pmod{q_n} \end{aligned} \qquad \text{or} \qquad \begin{aligned} x &\equiv -1 \pmod{q_1} \\ x &\equiv -2 \pmod{q_2} \\ &\ldots \\ x &\equiv -n \pmod{q_n} \end{aligned}$$

Large gaps in P_a-numbers

Theorem

For every a there are infinitely many bad primes $q_1, q_2, \ldots$.

Gaps in P_a

To find gaps of length n, find a number x which satisfies the conditions:

$$\begin{aligned} x+1 &\equiv 0 \pmod{q_1} \\ x+2 &\equiv 0 \pmod{q_2} \\ &\ldots \\ x+n &\equiv 0 \pmod{q_n} \end{aligned} \qquad \text{or} \qquad \begin{aligned} x &\equiv -1 \pmod{q_1} \\ x &\equiv -2 \pmod{q_2} \\ &\ldots \\ x &\equiv -n \pmod{q_n} \end{aligned}$$

The Chinese Remainder Theorem guarantees a solution for x since $q_1, \ldots, q_n$ are relatively prime. Then $x+1, \ldots, x+n$ are bad numbers.

Famous conjectures about prime numbers

Famous conjectures about prime numbers

Definition

A prime twin is a pair (p, q) of two consecutive prime numbers $p < q$ with $q - p = 2$, e.g. $(3, 5), (5, 7), (11, 13), ...)$.

Famous conjectures about prime numbers

Definition

A prime twin is a pair (p, q) of two consecutive prime numbers $p < q$ with $q - p = 2$, e.g. $(3, 5), (5, 7), (11, 13), ...)$.

Twin-prime-conjecture

There are infinitely many prime twins.

Famous conjectures about prime numbers

Definition

A prime twin is a pair (p, q) of two consecutive prime numbers $p < q$ with $q - p = 2$, e.g. $(3, 5), (5, 7), (11, 13), \ldots)$.

Twin-prime-conjecture

There are infinitely many prime twins.

Goldbach's conjecture (Goldbach, Euler 1742)

Every even number $n \geq 4$ can be expressed as sum of two prime numbers.

Twins in the sets P_a

Twins in the sets P_a

a\n	10	100	1000	10000	100000	1000000	10000000
2	2	13	55	347	2439	17903	140888
3	2	6	35	216	1438	10737	84069
4	0	0	0	0	0	0	0
5	1	7	33	228	1771	13522	109057
6	0	4	24	142	978	7223	56651
7	2	9	39	202	1397	10115	78652
8	2	13	55	347	2439	17903	140888
9	0	0	0	0	0	0	0
10	0	5	27	178	1284	9346	74137
11	1	8	60	317	2279	17229	136758
12	1	5	27	156	1014	7256	55479
13	1	6	30	179	1196	9030	71006
14	2	15	65	404	2757	20449	159570
15	1	5	28	189	1300	9998	79184
16	0	0	0	0	0	0	0
17	2	14	68	420	2984	22590	178247
18	0	3	25	172	1213	8906	69981

Twins in the sets P_a

Twins in the sets P_a

Results

Twins in the sets P_a

Results

- P_a contains no twins if a is a perfect square

Twins in the sets P_a

Results

- P_a contains no twins if a is a perfect square (proven).

Twins in the sets P_a

Results

- P_a contains no twins if a is a perfect square (proven).
- P_a contains infinitely many twins if a is no perfect square

Twins in the sets P_a

Results

- P_a contains no twins if a is a perfect square (proven).
- P_a contains infinitely many twins if a is no perfect square (conjectured).

Goldbach's conjecture with P_a-numbers

Goldbach's conjecture with P_a-numbers

In certain cases there is a analogue of the Goldbach's conjecture for P_a-numbers.

Outlook

Outlook

Fermat prime numbers

Define $Q_d := \{a \mid \exists\, n : d \mid a^n + 1\}$ for every $d \geq 2$.

Outlook

Fermat prime numbers

Define $Q_d := \{a \mid \ \exists\, n : d \mid a^n + 1\}$ for every $d \geq 2$. Looking for those d with large sets Q_d leads to Fermat prime numbers $2^{2^n} + 1$.

Soli Deo Gloria!

Thank you for your attention!