Relating $N\pm 1$ to the Primality of N

Nate Fulto

Definitions

Sequence Example

Theorem 1

Theorem 1

Theorem 13

N _ 1

N+1

TI.

Relating $N\pm 1$ to the Primality of N

Nate Fulton

May 6, 2015

Definitions

Example

Theorem 1

Theorem 13

N _ 1

Example

N + 1 Exampl

Thanks

Let N denote an odd integer > 1. Note that if an integer p is prime, then the following holds for every a:

$$a^{p-1} \equiv 1 \; (\bmod \; p)$$

Let N denote an odd integer > 1. Note that if an integer p is prime, then the following holds for every a:

$$a^{p-1} \equiv 1 \; (\bmod \; p)$$

In general, however, satisfaction of this congruence is not strong enough to imply primality.

Theorem 1

Theorem 13

N - 1 Example

. N + 1

LAampie

Let N denote an odd integer > 1. Note that if an integer p is prime, then the following holds for every a:

$$a^{p-1} \equiv 1 \; (\bmod \; p)$$

In general, however, satisfaction of this congruence is not strong enough to imply primality.

Example

Let N = 124, a = 5. 124 is not prime, but

$$5^{123} \equiv 1 \; (\bmod \; 124)$$

Relating $\mathit{N}\pm 1$ to the Primality of N

Nate Fulton

Definitions

Example

Theorem 1

TI........... 12

.. .

N + 1

Thank

Let N denote an odd integer > 1. Note that if an integer p is prime, then the following holds for every a:

$$a^{p-1} \equiv 1 \; (\bmod \; p)$$

In general, however, satisfaction of this congruence is not strong enough to imply primality.

Example

Let N = 124, a = 5. 124 is not prime, but

$$5^{123} \equiv 1 \pmod{124}$$

Definition

N is a pseudoprime base a (denoted psp base a) if it satisfies the congruence:

$$a^{N-1} \equiv 1 \pmod{N}$$

Relating $N\pm 1$ to the Primality of N

Definitions

In the N+1 case, we must look at Lucas sequences.

Definition

Let P and Q be integers such that the discriminant

$$D=P^2-4Q\neq 0$$

Nate Fultor

Definitions

Sequence Example

Theorem 1

Theorem 13

N — 1

N+1

Thank

In the N+1 case, we must look at Lucas sequences.

Definition

Let P and Q be integers such that the discriminant

$$D=P^2-4Q\neq 0$$

A Lucas sequence $\{U_k\}$ is defined as follows:

$$U_0=0,\,U_1=1$$

$$U_{k+2} = PU_{k+1} - QU_k$$

Relating $\mathit{N}\pm 1$ to the Primality of N

Definitions

Sequence Example

Theorem 1

Theorem 13

Λ/ 1

N + 1 Example

Thank

In the N+1 case, we must look at Lucas sequences.

Definition

Let P and Q be integers such that the discriminant

$$D=P^2-4Q\neq 0$$

A Lucas sequence $\{U_k\}$ is defined as follows:

$$U_0 = 0, U_1 = 1$$

$$U_{k+2} = PU_{k+1} - QU_k$$

We also define the Jacobi symbol:

$$\left(\frac{D}{N}\right) = \begin{cases} 1 & \text{if } D \text{ is a square (mod } N) \text{ i.e. } D \equiv a^2 \text{ for some } a \\ -1 & \text{if } D \text{ is not a square (mod } N) \\ 0 & \text{if } N \text{ divides } D \end{cases}$$

Sequence Example

Theorem 1

N — 1

Example

N+1

Thanks

Fact: If $p \nmid 2Q$, then $p \mid U_{p-\left(\frac{D}{p}\right)}$

Nate Fultor

Sequence Example

Theorem 1

Theorem 13

A/ 1

Example

Th. . . . 1.

Example

Let $P=1,\,Q=-3.$ Then D=13. The sequence starts:

N + 1 Exampl

Thank:

Fact: If $p \nmid 2Q$, then $p \mid U_{p-\left(\frac{D}{p}\right)}$

Example

Let P = 1, Q = -3. Then D = 13. The sequence starts:

k: 0 1 2 3 4 5 6 7 8 9 10 Uk: 0 1 1 4 7 19 40 97 217 508 1159

N+1Example

Thanks

Fact: If $p \nmid 2Q$, then $p \mid U_{p-\left(\frac{D}{p}\right)}$

Example

Let P = 1, Q = -3. Then D = 13. The sequence starts:

k : 0 1 2 3 4 5 6 7 8 9 10 *U_k* : 0 1 1 4 7 19 40 97 217 508 1159

5 exhibits the behavior above, as $5 \nmid 6$, $\left(\frac{13}{5}\right) = -1$, and $5 \mid 40$.

Fact: If $p \nmid 2Q$, then $p \mid U_{p-\left(\frac{D}{p}\right)}$

Example

Let P = 1, Q = -3. Then D = 13. The sequence starts:

 $k : 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10$ $U_k : 0 \quad 1 \quad 1 \quad 4 \quad 7 \quad 19 \quad 40 \quad 97 \quad 217 \quad 508 \quad 1159$

5 exhibits the behavior above, as $5 \nmid 6$, $\left(\frac{13}{5}\right) = -1$, and $5 \mid 40$. Similarly, $7 \nmid 6$, $\left(\frac{13}{7}\right) = -1$, and $217 = 7 \cdot 31$.

Fact: If $p \nmid 2Q$, then $p \mid U_{p-\left(\frac{D}{p}\right)}$

Example

Let P = 1, Q = -3. Then D = 13. The sequence starts:

$$k:0$$
 1 2 3 4 5 6 7 8 9 10 $U_k:0$ 1 1 4 7 19 40 97 217 508 1159

5 exhibits the behavior above, as $5 \nmid 6$, $\left(\frac{13}{5}\right) = -1$, and $5 \mid 40$. Similarly, $7 \nmid 6$, $\left(\frac{13}{7}\right) = -1$, and $217 = 7 \cdot 31$.

When looking at N+1, we will choose D such that $\left(\frac{D}{N}\right)=-1$, so knowing that $N\mid U_{N+1}$ is analogous to knowing that p is psp base a, where $N\mid a^{N-1}-1$.

Relating $N\pm 1$ to the Primality of N

Nate Fulto

Definition

Sequence Example

Theorem 1

Theorem 12

N - 1

N + 1

TI.

Suppose we have factored ${\it N}-1$ completely.

Theorem 1

Theorem 13

N — 1

Example

N+1Example

Thanks

Suppose we have factored N-1 completely. If for each p_i dividing N-1 there exists an a_i such that N is psp base a_i , but

$$a_i^{\frac{N-1}{p_i}} \not\equiv 1 \pmod{N}$$

then N is prime.

Sequence Example

Theorem 1

Theorem 13

LAdilip

Examp

[hankel

Suppose we have factored N+1 completely, and consider the set $\mathcal U$ of Lucas sequences $\{U_k^{(i)}\}$ whose shared discriminant D satisfies

$$\left(\frac{D}{N}\right) = -1$$

Suppose we have factored N+1 completely, and consider the set $\mathcal U$ of Lucas sequences $\{U_k^{(i)}\}$ whose shared discriminant D satisfies

$$\left(\frac{D}{N}\right) = -1$$

If for each q_m dividing N+1 there exists a Lucas sequence $U_k^{(m)} \in \mathcal{U}$ such that

$$N \mid U_{N+1}^{(m)}$$

but

$$N \nmid U_{\frac{N+}{q_m}}^{(m)}$$

then N is prime.

Sequence

Theorem 1

N-1

Example

Example

Let $N = 2^{30} + 7 = 1073741831$.

Theorem 1

Theorem 13

N — 1 Example

N+1

Thanks

Let $N=2^{30}+7=1073741831.$ Then $N-1=2\cdot 5\cdot 7\cdot 1901\cdot 8069.$

Example

-. .

Let $N = 2^{30} + 7 = 1073741831$.

Then $N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$.

It is relatively easy to check that N is psp base 2 and base 7.

Now, we satisfy the condition of Theorem 1 for each prime dividing ${\it N}-1$:

Let $N = 2^{30} + 7 = 1073741831$.

Then $N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$.

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$

Let
$$N = 2^{30} + 7 = 1073741831$$
.

Then
$$N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$$
.

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$

Let $N = 2^{30} + 7 = 1073741831$.

Then $N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$.

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$

Let
$$N = 2^{30} + 7 = 1073741831$$
.

Then
$$N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$$
.

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{1901}} \equiv 954146440 \not\equiv 1 \pmod{N}$$

Let
$$N = 2^{30} + 7 = 1073741831$$
.

Then
$$N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$$
.

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{1901}} \equiv 954146440 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{8069}} \equiv 905900321 \not\equiv 1 \pmod{N}$$

Let
$$N = 2^{30} + 7 = 1073741831$$
.

Then
$$N - 1 = 2 \cdot 5 \cdot 7 \cdot 1901 \cdot 8069$$
.

It is relatively easy to check that N is psp base 2 and base 7. Now, we satisfy the condition of Theorem 1 for each prime dividing N-1:

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{1901}} \equiv 954146440 \not\equiv 1 \pmod{N}$$

$$2^{\frac{N-1}{8069}} \equiv 905900321 \not\equiv 1 \pmod{N}$$

We conclude that N is prime.

N+1Example

Theorem 1

Theorem 13

N — 1

N + 1

Example

Let $N = 2^{30} + 33 = 1073741857$. Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

N+1Example

Let $N = 2^{30} + 33 = 1073741857$. Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$. We choose D=5 and get $\left(\frac{5}{N}\right)=-1$. Theorem 1

Theorem 13

N — 1

N + 1 Example

Thanks

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{N+1}$:

N — 1

Example

N + 1 Example

Thanks

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{N+1}$:

For q=2, the sequence with P=5, Q=5 works.

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{N+1}$:

For q=2, the sequence with P=5, Q=5 works.

For q=7, the sequence with P=9, Q=19 works.

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{\frac{N+1}{2}}$:

For q = 2, the sequence with P = 5, Q = 5 works.

For q = 7, the sequence with P = 9, Q = 19 works.

For q=7333 and q=10459, the Fibonacci numbers (P=1, Q=-1) work.

Relating $\mathit{N}\pm 1$ to the Primality of N

Nate Fulton

Sequence

Theorem 1

i neorem 13

N — 1

N+1 Example

Thank

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{\frac{N+1}{q}}$:

For q = 2, the sequence with P = 5, Q = 5 works.

For q = 7, the sequence with P = 9, Q = 19 works.

For q = 7333 and q = 10459, the Fibonacci numbers (P = 1,

Q=-1) work.

As an example of what it means to "work," consider the last prime. What we are saying is that $N \nmid U_{\frac{N+1}{10459}} = U_{102662}$.

Relating $\mathit{N}\pm 1$ to the Primality of N

Nate Fulton

. . . .

Sequence Example

Theorem 1

Theorem 13

N — 1

N + 1 Example

Thank

Let $N = 2^{30} + 33 = 1073741857$.

Then $N + 1 = 2 \cdot 7 \cdot 7333 \cdot 10459$.

We choose D=5 and get $\left(\frac{5}{N}\right)=-1$.

For each of the primes q dividing N+1, we must choose P and Q such that $N \mid U_{N+1}$, but $N \nmid U_{\frac{N+1}{a}}$:

For q = 2, the sequence with P = 5, Q = 5 works.

For q=7, the sequence with P=9, Q=19 works.

For q = 7333 and q = 10459, the Fibonacci numbers (P = 1, Q = -1) work

Q=-1) work.

As an example of what it means to "work," consider the last prime. What we are saying is that $N \nmid U_{\frac{N+1}{10459}} = U_{102662}$. Since we have a working sequence for each of the primes dividing N+1, we conclude that N is prime.

N+1Example

Relating $N\pm 1$ to the Primality of N

Definitions

Sequence Example

Theorem 1

Theorem 1

Λ/ 1

N + 1 Example

Thanks

For fun, here is the 102662nd Fibonacci number:

9.000002239 (440) 92.0000 (240) 100000 (440) 111 (270) 10000 (450) 117 (450) 10000 (450) 117 (450) 10000 (450) 117 (450) 10000 (450) 117 275 THE LOSE SCHOOL TO PRODUCE THE STREET OF 2014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 1014 | 10 804401342902031000787953925171129774315994117027024102491799585142949923312441024491194592982443125302246149422876574142570273112419724767524777390314 867.756((1985)5581)3447-05/(1985)35((19

Nate Fultor

Definitions

Sequence Example

Theorem 1

Theorem 13

V — 1

N + 1

Thanks!

New Primality Criteria and Factorizations of $2^m \pm 1$ John Brillhart, D. H. Lehmer and J. L. Selfridge Mathematics of Computation Vol. 29, No. 130 (Apr., 1975) , pp. 620-647 Published by: American Mathematical Society Stable URL: http://www.jstor.org/stable/2005583