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

Nate Fulton

May 6, 2015

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

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

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

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

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

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

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

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

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

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

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

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:

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

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

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

Definition

Let P and Q be integers such that the discriminant

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

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:

$$U_0 = 0, U_1 = 1$$

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

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:

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

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

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:

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

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	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 $217 = 7 \cdot 31$.

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 $N \mid a^{N-1} - 1$.

Suppose we have factored $N - 1$ completely.

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.

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

$$N \nmid U_{\frac{N+1}{q_m}}^{(m)}$$

then N is prime.

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

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

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 $N - 1$:

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 $N - 1$:

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

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 $N - 1$:

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

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 $N - 1$:

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$

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 $N - 1$:

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{1901}} \equiv 954146440 \not\equiv 1 \pmod{N}$$

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 $N - 1$:

$$7^{\frac{N-1}{2}} \equiv 1073741830 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{5}} \equiv 785229716 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{7}} \equiv 507218236 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{1901}} \equiv 954146440 \not\equiv 1 \pmod{N}$$
$$2^{\frac{N-1}{8069}} \equiv 905900321 \not\equiv 1 \pmod{N}$$

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 $N - 1$:

$$
\begin{aligned}
7^{\frac{N-1}{2}} &\equiv 1073741830 \not\equiv 1 \pmod{N} \\
2^{\frac{N-1}{5}} &\equiv 785229716 \quad \not\equiv 1 \pmod{N} \\
2^{\frac{N-1}{7}} &\equiv 507218236 \quad \not\equiv 1 \pmod{N} \\
2^{\frac{N-1}{1901}} &\equiv 954146440 \quad \not\equiv 1 \pmod{N} \\
2^{\frac{N-1}{8069}} &\equiv 905900321 \quad \not\equiv 1 \pmod{N}
\end{aligned}
$$

We conclude that N is prime.

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

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

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

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 $N \nmid U_{\frac{N+1}{q}}$:

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.

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.

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.

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 $N \nmid U_{\frac{N+1}{10459}} = U_{102662}$.

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 $N \nmid U_{\frac{N+1}{10459}} = U_{102662}$.
Since we have a working sequence for each of the primes dividing $N + 1$, we conclude that N is prime.

For fun, here is the 102662$^{\text{nd}}$ Fibonacci number:

For fun, here is the 102662^{nd} Fibonacci number:

[illegible]

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