Using Lucas Sequences in Primality Testing

Karl Heimbuck
Dr. Siguna Mueller
Department of Mathematics
EPSCoR/Honors Program

Why do we need prime numbers?

- Digital security
- Public-key cryptography

Fermat's Little Theorem

- If *p* is a prime number and *a* is an integer, then:
  - $a^{p-1} \equiv 1 \bmod p$ if $\gcd(a,p) = 1$
  - This holds for all primes but some composites as well.

Pseudoprimes: What are they?

- A pseudoprime fulfills a primality test but is in fact a composite.

- 561, which is composite, passes the Fermat test as a prime would
  - $2^{560} \equiv 1 \bmod 561$
  - $561 = 3 * 11 * 17$

Carmichael Numbers

- Properties
  - If a prime number p is a factor of the Carmichael number n, then $p - 1 \mid n - 1$.
  - Squarefree
  - Have at least 3 prime factors

- Carmichael numbers fulfill the Fermat test for any base a such that $\gcd(a,n) = 1$.

- The Fermat test is not good enough!

Refinements of FLT

- $a^{(p-1)/2} \equiv 1 \bmod p$
- Miller-Rabin Test
- The Miller-Rabin test works very well in practice but could still be improved upon.

Lucas Sequences

- Let P and Q be integers and $D = P^2 - 4Q$

- List of U's and V's such that
  - $U_n = PU_{n-1} - QU_{n-2}$
  - $V_n = PV_{n-1} - QV_{n-2}$

- Initial terms
  - $U_0 = 0$
  - $U_1 = 1$
  - $V_0 = 2$
  - $V_1 = P$

Example of a Lucas Sequence

$P = 2$ and $Q = -1$

$U_0 = 0$

$U_1 = 1$

$U_2 = 2$

$U_3 = 5$

$U_4 = 12$

$U_5 = 29$

$U_6 = 70$

$U_7 = 169$

$U_8 = 408$

$V_0 = 2$

$V_1 = 2$

$V_2 = 6$

$V_3 = 14$

$V_4 = 34$

$V_5 = 82$

$V_6 = 198$

$V_7 = 478$

$V_8 = 1154$

Initial observations

- $U_{n+1} \equiv 0 \bmod n$

  OR

- $U_{n-1} \equiv 0 \bmod n$

- $U_n \equiv \pm 1 \bmod n$

- $V_n \equiv 2 \bmod n$

- $V_{n+1} \equiv P \bmod n$

  OR

- $V_{n-1} \equiv P \bmod n$

Example

- For $P = 2$ and $Q = -1$, test $n = 7$ for primality
- $U_7 = 169$
  - $U_{n+1} = U_8 = 408 \equiv 2 \bmod 7$
  - $U_{n-1} = U_6 = 70 \equiv 0 \bmod 7$
  - $U_n = U_7 = 169 \equiv 1 \bmod 7$
- $V_7 = 478$
  - $V_7 = 478 \equiv 2 \bmod 7$
  - $V_8 = 1154 \equiv 6 \bmod 7$
  - $V_6 = 198 \equiv 2 \bmod 7$ (where P = 2)

Question

- Can we refine the conditions to know when we have +1 and when we have -1?

- Let's make use of the discriminant $D = P^2 - 4Q$ by looking at the Legendre/Jacobi symbol, denoted ε.
  - $\varepsilon = 1$ if D is a square modulo n
  - $\varepsilon = -1$ if D is not a square modulo n

Refined Lucas tests

- Test 1: $U_{n-\varepsilon} \equiv 0 \bmod n$
- Test 2: $U_n \equiv \varepsilon \bmod n$
- Test 3: $V_n \equiv 2 \bmod n$
- Test 4: $V_{n-\varepsilon} \equiv P \bmod n$

Pseudoprime Trouble!

- Let's test $n = 341$ for primality using Test 2 with $P = 2$ and $Q = 4$.
  - $\varepsilon = -1$
  - $U_{341} = -223974474217780421055744228056844427812164549723464953489998910009637918711801609453808774932716071157776$

    $U_{341} \equiv -1 \bmod 341$
  - 341 passes Test 2 as a prime number
  - $341 = 11 * 31$

- Does the same pseudoprime pass both Test 1 and Test 2?

More Trouble!

- Let's test $n = 341$ using Test 1
  - $U_{n-\varepsilon} = U_{n-(-1)} = U_{342} \equiv 0 \bmod 341$
- 341 passes Test 1 as well
- Let's go on to Test 3

Out of the woods!

- What about Test 3?
  - $V_{341} \equiv 219 \bmod 341$
  - Does not pass Test 3 so 341 must be composite.

- We can combine the Lucas tests to create a more refined primality test.

- Which combination works best?
  - Doesn't seem to be a most effective combination.
  - Results seemed to favor a combination of one of the tests on V with one of the tests on U but this cannot be proven.

What if we combine a Lucas test with the Fermat test?

- 88831 passes all of the tests for $P = 2$ and $Q = -4$
- $88831 = 211 * 421$
- Does not pass the Fermat test when using 2 as our base, $2^{88830} \equiv 87988 \bmod 88831$

Which combinations work best?

- Would not want to use Test 1 and the Fermat test together because they essentially end up testing the same condition when $\varepsilon = -1$.

- Aside from avoiding that there does not seem to be a best combination of Fermat with any of the other 3 tests.

Stronger Conditions

- If $\varepsilon = \left(\frac{Q}{n}\right) = -1$ and n is a prime number, then $U_{(n-\varepsilon)/2} \equiv 0 \mod n$.

- If $\varepsilon = \left(\frac{Q}{n}\right) = 1$ and n is a prime number, then $V_{(n-\varepsilon)/2} \equiv 0 \mod n$.

- Did not extensively test these.

What do we do with the Lucas pseudoprimes?

- Can we characterize them?
  - Doesn't seem that way.
  - But doing so would be a nice way to adjust the tests and assure that they do not slip through.

Conclusion

- The Lucas tests could be an effective primality testing tool but may still need a little tweaking.
- Combinations of a Lucas test with a Fermat test seem to work better than combinations of a Lucas test with another Lucas test.
- It is more effective to combine one Lucas test with the Fermat test than to combine two Lucas tests with the Fermat test.
  - Run time is much quicker
  - The payoff isn't significant

What's next?

- Can one characterize Lucas pseudoprimes?
- Will a certain base work best when using the Fermat test?
- Proposal by Bailie, Wagstaff, Pomerance and Selfride
  - Let $a = 2$, use the same ε as defined earlier, and a specific P and Q. It appears that there are no pseudoprimes for these conditions.
  - Do any exist or not?

Thanks!

- ESPCoR
  - Rick Matlock
  - Barbara Kissack
- Honors Program
- Dr. Mueller