**Complex Primitive Roots and Fermat Tests**

Let a + ib be a complex integer. (a and b are integers and i2 = -1.)

Let p be an odd prime. We say that g = a + ib is a complex primitive root of p if m = p2 – 1 is the smallest exponent such that

gm  ≡ 1 (mod p).

We say that a + ib ≡ c + id (mod N) if a ≡ c and b ≡ d.

**The Complex Fermat Theorem**

If gcd(p, a2 + b2) = 1, where p is prime, then

(1) (a + ib)(p-1)(p+1) ≡ 1 (mod p).

If p’s primality is unknown, then (1) is strong evidence that p is prime.

When p ≡ 3 (mod 4), a stronger theorem than (1) is true.

**Complex Fermat Theorem for Blum primes**

Let p be a prime of the form 4k + 3. If a and b are distinct, and 0 < a, b < p, and a + b ≠ n, then

(2) (a + ib)(p+1)/2 ≡ c + id (mod p), where cd = 0 and c2 + d2 > 0.

Primes of the form 4k + 3 are called Blum primes, and we have encountered them before in connection with finding square roots modulo p. They have a simple formula for finding square roots (problem 1 in Homework 4.) Safe primes are also Blum primes.

**Primality Testing**

If p ≡ 3 (mod 4) and (2) holds, this is strong evidence that p is a prime.

**Carmichael Numbers**

In 1910 Robert Carmichael discovered that the number p = 561 = 3 X 187 satisfies

(3) ap ≡ a (mod p) for all a ϵ (0, p) that are coprime to p. This is another form of Fermat’s theorem.

In his honor we define a Carmichael number to be any number n such that bn ≡ b (mod n) for all numbers b coprime to n. The number 561 is the smallest Carmichael number. The pattern is that n = qrs where q, r, and s are distinct primes and q-1|n-1, r-1|n-1, and s-1|n-1. In other words, n is a Carmichael number if and only if n = qrs, where q, r and s are distinct primes, and

q-1|n-1

r-1|n-1 and

s-1|n-1.

For example, 561 = 3 X 11 X 17.

Check:

3-1|561-1 🡨 2|560

11-1|560 🡨 10|560

17-1|560 🡨 16|560 🡨8|280 🡨 4|140 🡨 2|70 🡨 1|35

A subset of the Carmichael numbers are the numbers of the form p = (6k + 1)(12k + 1)(18k + 1) for which the three factors are all prime. This is a small subset of the set of all Carmichael numbers, because the same parameter k appears in all three primes.

Easy to check:

If n = (6k+1)(12k+1)(18k+1),

Then we need that

6k|n-1

12k|n-1

18k|n-1

LCM[6, 12, 18]k | n-1

36k | n-1

n = (6k + 1)(12k + 1)(18k + 1) = (6X12X18)k3 + (6X12 + 6X18 + 12X18)k2 + (6+12+18)k + 1

n-1 = 1296k3 + 396k2 + 36k

n-1 = (1296k2 + 396k + 36)k

We want

6k | n-1 🡨 6|1296k2 + 396k + 36 yes.

12k|n-1 🡨 12|1296k2 + 396k + 36 yes.

18k | n-1 🡨 18|1296k2 + 396k + 36 yes.

Let’s find one

k 6k+1 12k+1 18k+1 All primes? n

1 7 13 19 yes 1729

2 13 25 no

3 19 37 55 no

4 25 no

5 31 61 91 no

6 37 73 109 yes 294409

After extensive experimentation, Boris S. Verkhovsky did not find a single Carmichael number of the form 4k+3 that satisfied (2). This suggests that the complex Fermat test could be a useful supplement to the Fermat test.

**Details**

Boris tested all of the 246,683 Carmichael numbers that are less than 1016, using test (2) on those that were of the form 4k+3. For numbers of the form 4k+1, he used the following test.

**Complex Fermat Test for primes p = 4k+1**

Let p be a prime p = 4k+1. Let a and b be distinct and 0 < a, b < p. Then

(4) (a + ib)(p – 1)/2 ≡ c + id (mod p), where cd = 0 and c2 + d2 > 0.

The experiment only used a small number of values for a + ib, due to limitations of time.

**Results**

Not a single Carmichael number of the form 4k+3 passed test (2).

A small number of Carmichael numbers of the form 4k+1 passed test (4).

**Future Research**

Boris’s experiments suggest that numbers having a high probability of fooling a Fermat test may have a low probability of fooling a complex Fermat test.

**Notation**

Let n be a composite number and let b be chosen at random. Then the probability that

bn-1 ≡ 1 (mod n) is |{a : an-1 ≡ 1 (mod n)}|/n. Let’s denote this by F(n) for Fermat test.

Similarly, the probability that

(\*) (a + ib)(n+1)(n-1) ≡ 1 (mod n) is the number of elements a + ib such that (\*) holds divided by n2. Denote

this by CF(n) for Complex Fermat test.

Boris’s experiments show that numbers n for which F(n) is extremely high, namely the Carmichael numbers have very low values of CF(n).

**Question**

Is it the case that a high value for F(n) correlates with a low value of CF(n)?

This might take the form of a formula, such as

F(n) + CF(n) < 1, or

F(n)\*CF(n) < ½ or some such.

**Another Question**

How does the Rabin equivalent of the Complex Fermat test behave?

In computing (a+ib)(p-1)(p+1) (mod p) and getting 1 as the answer, we can say that if p is a prime, and if

(p-1)(p+1) = 2km, where m is odd, then one of the numbers d ≡ (a+ib)m, d2%p, d4%p, d8%p, … will be a square root of 1 that is not itself 1. If p really is a prime, then that number had better be -1 ≡ p-1, and this will provide a Rabin-like test for primality. Will the probability of fooling this test be less than or equal to ¼ as in the real Rabin Test?