UTILILIZING CAS TECHNOLOGY TO EXPLORE FACTORING AND PRIMALITY

Jay L. Schiffman

Rowan University

201 Mullica Hill Road

Glassboro, NJ 08028-1701

schiffman@rowan.edu

Abstract: The primes encompass the atoms of the natural number system. In this session, participants will use CAS technology with the TI-89/VOYAGE 200 to determine the primality of integers and explore Fermat's Method of Factorization and the Lucas-Lehmer Test for Mersenne primes. In addition, a number of Fibonacci and Lucas numbers will be factored.

Questions involving primality have fascinated both professional and amateur mathematicians throughout the rich history of the subject. In the appropriate settings, Fermat's Method of Factorization, The Lucas-Lehmer Test associated with Mersenne numbers, and the primes in the Fibonacci and Lucas sequences have been the subject of much study and interest. We will delve into these ideas in this session and engage the participants.

Fermat's Method of Factorization is particularly useful when one wishes to factor large integers in which the prime factors are roughly of equal size. In Fermat's Method, for a given positive integer n, one seeks integers x *and* y such that $n = x^2 - y^2$. Then $n = (x-y)\cdot(x+y)$ (1) and n is factored. Every positive integer can be represented in the form $n = x^2 - y^2$ by writing $n = a \cdot b$

$(a > b)$ and note this yields

$a = x + y$ (2)
$b = x - y$ (3)

Adding and subtracting (2) and (3) and then solving for $x \text{ and } y$ in (4) and (5) gives us respectively

$$a+b=2\cdot x \;(4)$$
$$a-b=2\cdot y \;(5)$$

$$x=\frac{1}{2}\cdot(a+b)\;(6)$$
$$y=\frac{1}{2}\cdot(a-b)\;(7)$$

Hence $x^2-y^2=\frac{1}{4}\cdot\left[(a+b)^2-(a-b)^2\right]=a\cdot b.\;(8)$

As the initial trial for x, we try $x_1\left\lceil\sqrt{n}\right\rceil$ where $\lceil x\rceil=$ the ceiling function. $(\lceil x\rceil = \textit{the smallest integer} \geq x\ (x\in\mathbb{R}))$. Now check if $\Delta x_i = x_i^2 - n$ is a perfect square. There are only 22 combinations of the last two digits which a square number can assume so most combinations can be eliminated. Stop when a square number can be obtained.

In 1876, Edouard Lucas discovered a fast way to test the primality of a Mersenne number. Mersenne numbers are of the form $M_n=2^n-1$ where n is a positive integer. Using the test and calculators, several primes were added to the list of Mersenne primes. In 1930, D.H. Lehmer published an improved version of Lucas' algorithm. *The Lucas-Lehmer Test* for primality follows: Let $u(1)=4$. For $i=0\ to\ i=p-2$, compute $u(i+1)=\left(u(i)^2-2\right)\bmod M_p\ \textit{iff}\ u(p-1)=0$, then M_p is a prime, where the "$\bmod M_p$" means to keep only the remainder after division by M_p. By way of an example, let us apply the Lucas-Lehmer Test on $M_5=31$.

$$u(1)=4; u(2)=\left(4^2-2\right)\bmod 31=14; u(3)=\left(14^2-2\right)\bmod 31=8;$$
$$u(4)=\left(8^2-2\right)\bmod 31=0.$$

Hence M_5 is a prime number. One can utilize the TI-89 / VOYAGE 200 and apply the test on

$M_3, M_7, \textit{and } M_{11}$. $(M_{11}\ \textit{is not prime.})$

Other activities associated with prime numbers and factoring include the factoring of Fibonacci and Lucas Numbers. Determining whether a large positive integer is prime or composite is easy for technology to accomplish and can often be done in seconds. The prime factorization of large positive integers is an entirely different matter. This problem is classified as NP Hard and a calculating device could take centuries to factor a large composite integer. The key is the second largest prime factor. If that factor is large, one runs into difficulties. Examples will be provided. MATHEMATICA, a copyright of Wolfram Research Inc. is a very powerful CAS that can achieve far more computing power than even a fine CAS graphics calculator. As a postscript, participants will feel empowered by both the primes and factorization methods and hopefully this will serve as a springboard for discovering new insights with the aid of CAS technology.

Our first goal is to discover square numbers. This is central for Fermat's Method. A question arises as to which positive integers can be perfect squares in the sense that a necessary condition can be secured. One observes neat patterns in the prefect squares:

$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16,\ 5^2 = 25,\ 6^2 = 36,\ 7^2 = 49,\ 8^2 = 64,\ 9^2 = 81,\ 10^2 = 100,$

$11^2 = 121,\ 12^2 = 144,\ 13^2 = 169,\ 14^2 = 196,\ 15^2 = 225,\ 16^2 = 256,\ 17^2 = 289,\ 18^2 = 324,$

$19^2 = 361,\ 20^2 = 400.$

The pattern involving the unit's digits is quite clear. The sequence occurs in the pattern 1, 4, 9, 6, 5, 6, 9, 4, 1, 0 and then recycles in this form. Hence integers that constitute perfect squares necessarily terminate in the digits 0, 1, 4, 5, 6, or 9. (This condition, of course, is not sufficient. One only needs to examine the integers 21, 34, 59, 75, 86, and 200 and observe that they are not perfect squares). Thus integers terminating in the digits 2, 3, 5, or 8 cannot be square numbers. In addition, the pattern of units digits occurs as a palindrome in the sense of reading the same both backwards as well as forwards (i.e. one has 1 4 9 6 5 6 9 4 1 separated by a 0 before recycling in the same pattern. Thus our pattern is 1 4 9 6 5 6 9 4 1 0 1 4 9 6 5 6 9 4 1 0 1 4 9 6 5 6 9 4 1 0...). If the last two digits of an integer are to constitute a square number, then one of twenty-two possible scenarios must occur. This can be investigated via the VOYAGE 200 CAS manufactured by Texas Instruments Inc. We are inferring that there are only 22 combinations of the last two digits which a square number can assume, so most combinations can be eliminated. Stop when a square number is obtained. FIGURE 1 provides the squaring function in FUNCTION MODE, FIGURE 2 the TABLE SETUP and FIGURES 3-9 the TABLE:

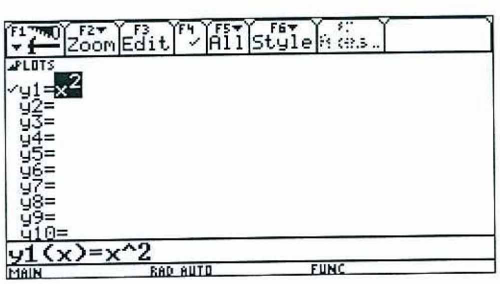


FIGURE 1 (Y=EDITOR)

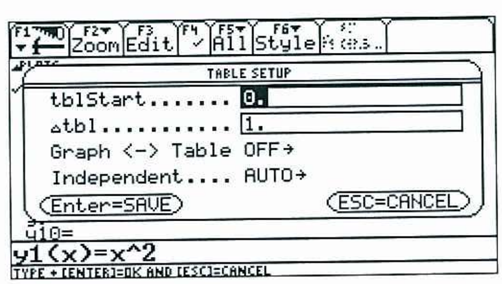
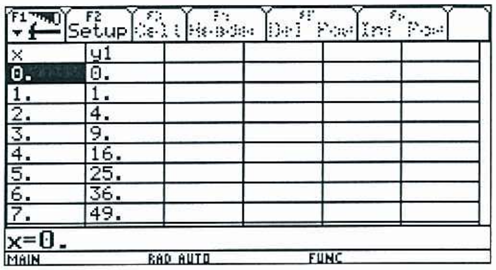
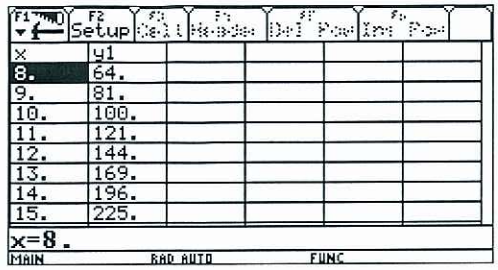


FIGURE 2 (TABLE SETUP)



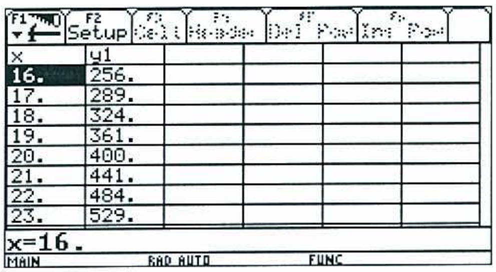
x	y1
0.	0.
1.	1.
2.	4.
3.	9.
4.	16.
5.	25.
6.	36.
7.	49.

FIGURE 3 (squares of integers 0-7)



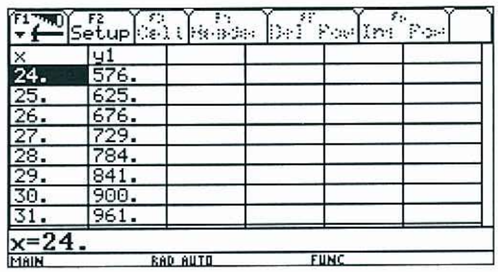
x	y1
8.	64.
9.	81.
10.	100.
11.	121.
12.	144.
13.	169.
14.	196.
15.	225.

FIGURE 4 (squares of integers 8-15)



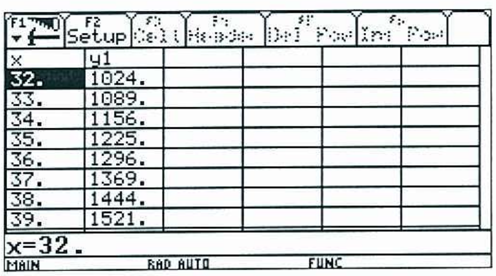
x	y1
16.	256.
17.	289.
18.	324.
19.	361.
20.	400.
21.	441.
22.	484.
23.	529.

FIGURE 5 (squares of integers 16-23)



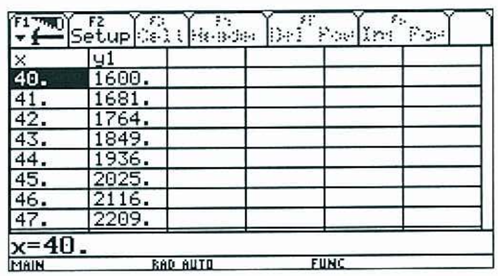
x	y1
24.	576.
25.	625.
26.	676.
27.	729.
28.	784.
29.	841.
30.	900.
31.	961.

FIGURE 6 (squares of integers 24-31)



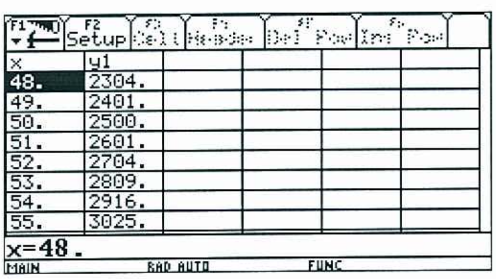
x	y1
32.	1024.
33.	1089.
34.	1156.
35.	1225.
36.	1296.
37.	1369.
38.	1444.
39.	1521.

FIGURE 7 (squares of integers 32-39)



x	y1
40.	1600.
41.	1681.
42.	1764.
43.	1849.
44.	1936.
45.	2025.
46.	2116.
47.	2209.

FIGURE 8 (squares of integers 40-47)



x	y1
48.	2304.
49.	2401.
50.	2500.
51.	2601.
52.	2704.
53.	2809.
54.	2916.
55.	3025.

FIGURE 9 (squares of integers 48-55)

From the FIGURES 3-9, we see that the last two digits for an integer that is potentially a perfect square are 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, and 96. We also observe that the cyclical pattern of the last two digits of the square of an integer commencing with 0 are 00, 01, 04, 09, 16, 25, 36, 49, 64, 81, 00, 21, 44, 69, 96, 25, 56, 89, 24, 61, 00, 41, 84, 29, 76, 25, 76, 29, 84, 41, 00, 61, 24, 89, 56, 25, 96, 69, 44, 21, 00, 81, 64, 49, 36, 25, 16, 09, 04, 01. We then repeat the cycle in the same fashion starting with 00. While one should think modulo 100, the period of the last two digits of the square of a number is 50. Also note that the first 25 follow a pattern and the last 25 reverse the pattern. For example, the last two digits of the twenty-sixth square number (76) are identical with the last two digits of the twenty-fourth square number.

Fermat's Method works most efficiently if the factors of n ($n = x \cdot y$) are relatively of the same size. If n is prime, then far too many trials are required. Consequently Fermat's method is highly inefficient. In addition, the factors of n need not be prime. The VOYAGE 200 will prove useful in these investigations. We conclude this section with two examples.

(a). Consider $n = 2047$ *where* $2047 = x^2 - y^2$. Thus $y^2 = x^2 - 2047$. Consider $\sqrt{2047} \approx 45.2437841035$. We examine the function $y = x^2 - 2047$. We view in FIGURE 10 the function and in FIGURE 11 the TABLE SETUP with the TABLE displayed in FIGURES 12-13:

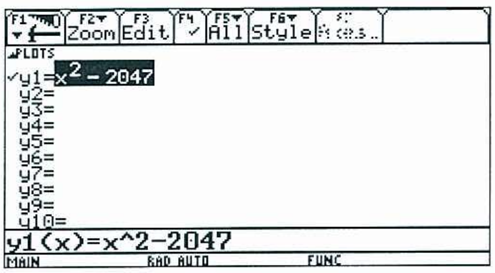


FIGURE 10 (Y= EDITOR)

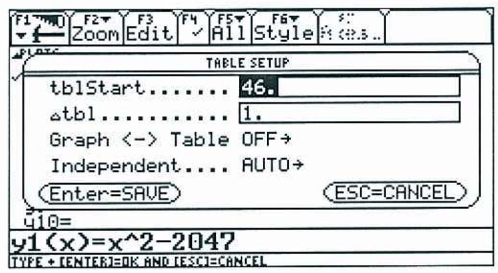
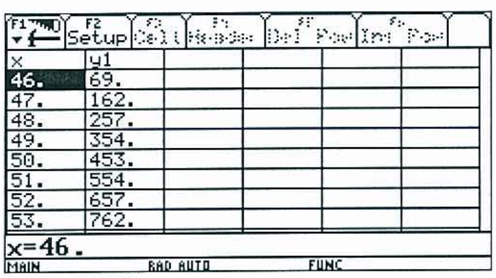


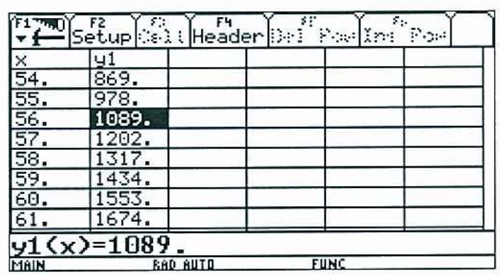
FIGURE 11 (TABLE SETUP)



x	y1
46.	69.
47.	162.
48.	257.
49.	354.
50.	453.
51.	554.
52.	657.
53.	762.

x=46.

FIGURE 12 (looking for first square)



x	y1
54.	869.
55.	978.
56.	1089.
57.	1202.
58.	1317.
59.	1434.
60.	1553.
61.	1674.

y1(x)=1089.

FIGURE 13 (found 1089 as the first square)

We seek the first integer in the table which is a perfect square. We immediately eliminate 162, 257, 354, 554, 453, 657, 762, and 978 from consideration; for 62, 57, 54, 53, 57, 62, and 78 cannot be the last two digits of a positive integer that is a perfect square. This leaves us with 69, 869 and 1089. 69 is clearly not a perfect square and neither is 869. On the other hand, $\sqrt{1089} = 33$. Thus 1089 is a perfect square found after eleven iterations. We have $n = 2047 = 56^2 - 1089 = 56^2 - 33^2 = (56-33)\cdot(56+33) = 23 \cdot 89$. Hence $2047 = 23 \cdot 89$. (Both factors are prime.)

(b). 23 is prime, but apply Fermat's Method. We consider $n = 23$ *where* $23 = x^2 - y^2$. Thus $y^2 = x^2 - 23$. Note that $\sqrt{23} \approx 4.79583152331$. See FIGURE 14. Examine the function $y = x^2 - 23$ in FIGURE 15 with the TABLE SETUP in FIGURE 16 and the TABLE in FIGURE 17 below:

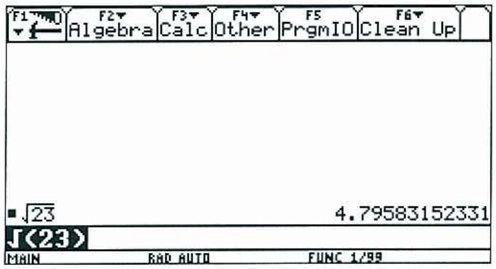


FIGURE 14 (approximation of $\sqrt{23}$)

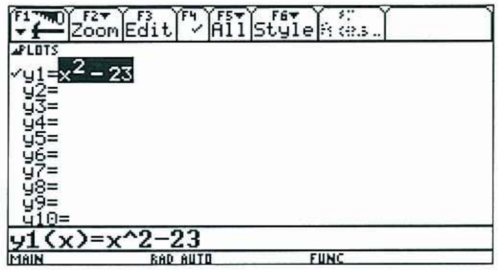


FIGURE 15 (Y= EDITOR)

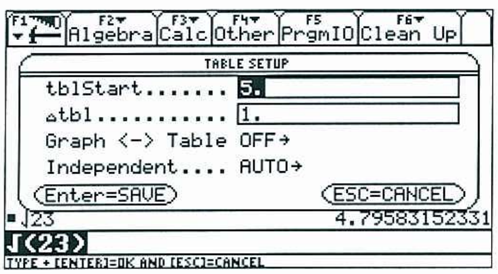


FIGURE 16 (TABLE SETUP)

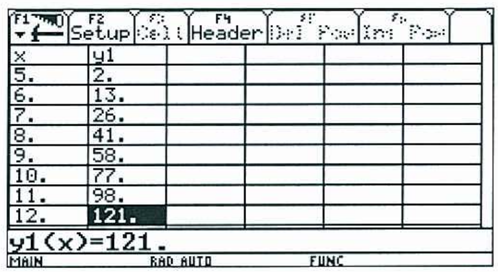
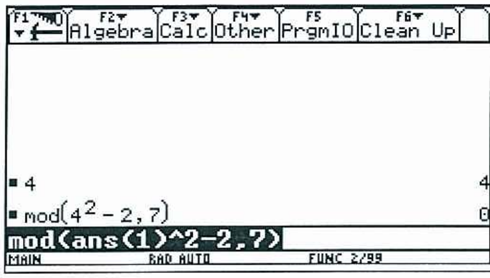


FIGURE 17 (121 is the first square)

Observe that the last two digits of a square cannot be 02, 13, 26, 58, 77, or 98 eliminating the integers 2, 13, 26, 58, 77, and 98 from consideration. Moreover, 41 is not a perfect square. 121 is a perfect square; for $121 = 11^2$, the initial perfect square in this list. One required 8 iterations to achieve this. While the process will always terminate in a perfect square, the method is inefficient. We have $n = 23 = 12^2 - 121 = 12^2 - 11^2 = (12-11)\cdot(12+11) = 1\cdot 23$ verifying that the integer 23 is prime.

Let us next apply the Lucas-Lehmer Test for primality on the Mersenne numbers $M_3 = 2^3 - 1 = 8 - 1 = 7, M_7 = 2^7 - 1 = 128 - 1 = 127,$ *and* $M_{11} = 2^{11} - 1 = 2048 - 1 = 2047.$

For $M_3 = 7, u(1) = 4$ *and* $u(2) = (4^2 - 2) \bmod 7 = 0.$ Hence M_3 is indeed prime. See FIGURE 20 below:



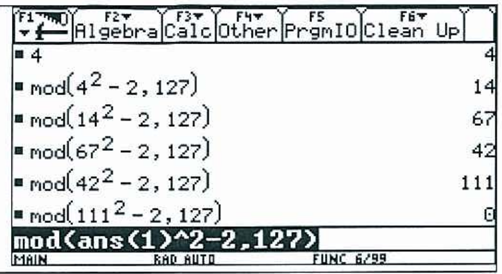
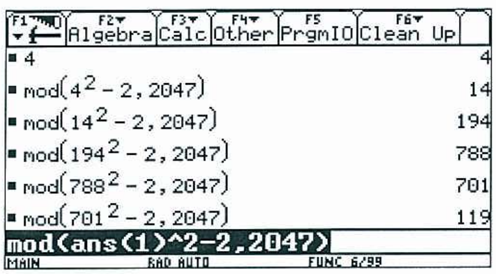


FIGURE 20 (Lucas-Lehmer Test on $M_3 = 7.$) FIGURE 21 (Lucas-Lehmer Test on $M_7 = 127.$)

For $M_{11} = 2047,$ consider the calculations in FIGURES 22-23 below:



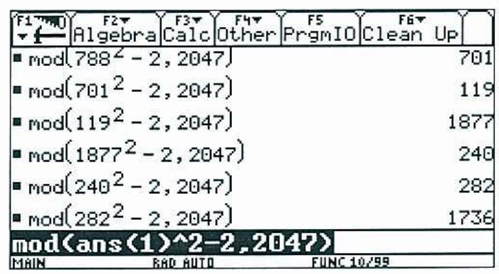


FIGURE 22 (Lucas-Lehmer Test on $M_{11} = 2047.$) FIGURE 23 (same as FIGURE 22)

For $M_{11} = 2047, p = 11 \Rightarrow p - 1 = 10$ and after 10 steps we do not obtain an output of 0 so that M_{11} is not prime. The Lucas-Lehmer Test is not very efficient for larger values of M_p and better tests must be devised. The GIMPS (Great Internet Mersenne Prime Search) is currently a very active area of number theory and one can join. Keep in mind that "prime does pay." The discovery of the thirty-eighth Mersenne prime netted the researcher $250,000!

We next consider the factorizations of Fibonacci and Lucas numbers. In order to generate the first of these sequences, recall the recursive definition of the Fibonacci sequence, $FIB(N)$ defined as follows:

$$FIB(1) = FIB(2) = 1$$
$$FIB(N) = FIB(N-2) + FIB(N-1) \text{ for } N \geq 3.$$

On the HOME SCREEN, we generate the Fibonacci sequence. We initialize the first two terms typing 1 each time followed by ENTER. On the third line, type $ans(2) + ans(1)$, then ENTER. Generate new terms of the sequence by consistently pressing ENTER.

We view the initial twenty-eight terms of the Fibonacci sequence in FIGURES 24-27 below:

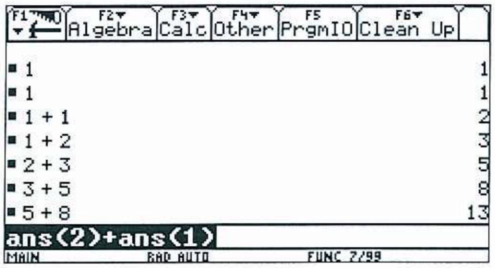


FIGURE 24 $(FIB(1) - FIB(7))$.

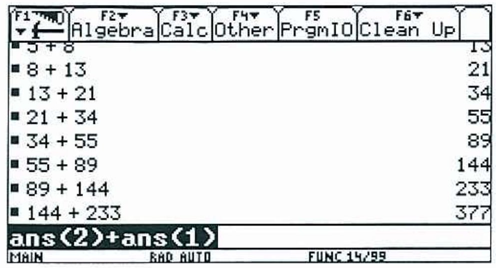


FIGURE 25 $(FIB(8) - FIB(14))$.

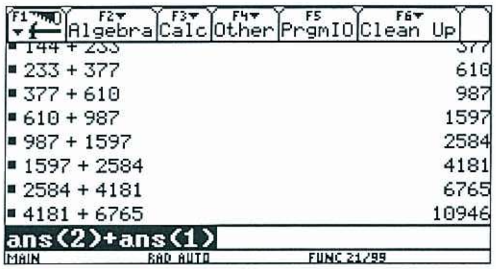


FIGURE 26 $(FIB(15) - FIB(21))$.

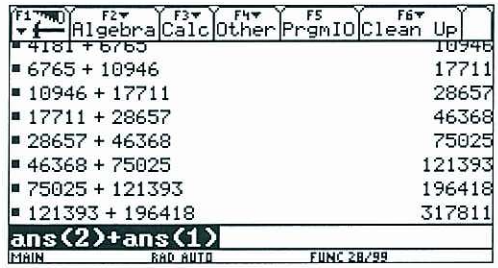


FIGURE 27 $(FIB(22) - FIB(28))$.

Let us next generate the initial eight Fibonacci primes. We proceed in the same fashion we generated the terms of the Fibonacci sequence, except we utilize the factor option. See FIGURES 28-31 below:

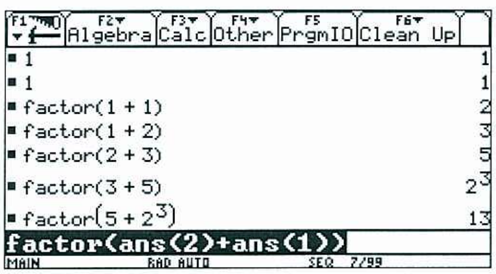


FIGURE 28 $(FIB(1) - FIB(7))$ factored.

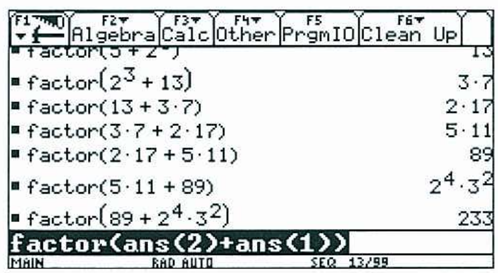


FIGURE 29 $(FIB(8) - FIB(13))$ factored.

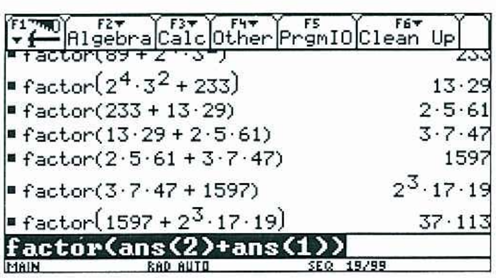


FIGURE 30 $(FIB(14) - FIB(19))$ factored

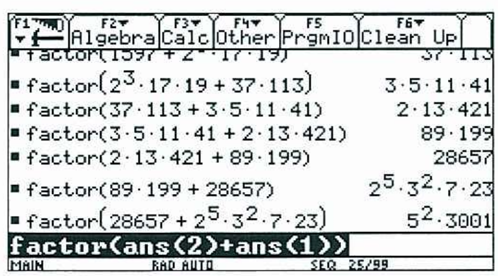


FIGURE 31 $(FIB(20) - FIB(25))$ factored.

The first number 7/99 at the bottom of the screen in FIGURE 28 indicates that the 7th entry in the Fibonacci sequence is 13. One can save up to 99 previous calculations in the history. See FORMAT which is F1 9. The initial ten Fibonacci primes are as follows:

$$FIB(3)=2, FIB(4)=3, FIB(5)=5, FIB(7)=13, FIB(11)=89,$$
$$FIB(13)=233, FIB(17)=1597, FIB(23)=28657.$$

Although there are infinitely many prime numbers as well as Fibonacci numbers, it remains open as to whether there are infinitely many Fibonacci primes. It is known that with the exception of $n=4$ (where $FIB(4)=3$, a prime), every other Fibonacci prime arises from $FIB(n)$ such that n is itself prime. The converse is not valid; 19 is prime but $FIB(19)=4181=37\cdot 113\,(composite)$.

In order to generate the Lucas sequence, recall the definition:

$$LUC(1)=1, LUC(2)=3$$
$$LUC(N)=LUC(N-2)+LUC(N-1)\ for\ N\geq 3.$$

In a manner analogous to the Fibonacci sequence in the previous problem, we generate the initial twenty-eight terms of the Lucas sequence on the HOME SCREEN in FIGURES 32-35 below:

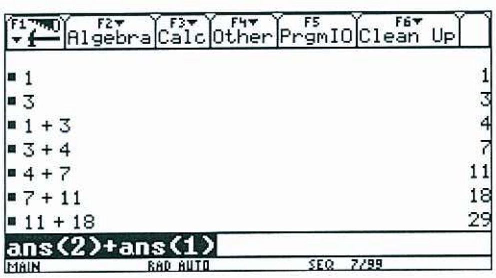


FIGURE 32 $(LUC(1)-LUC(7))$.

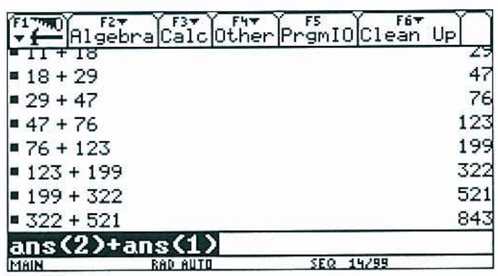


FIGURE 33 $(LUC(8)-LUC(14))$.

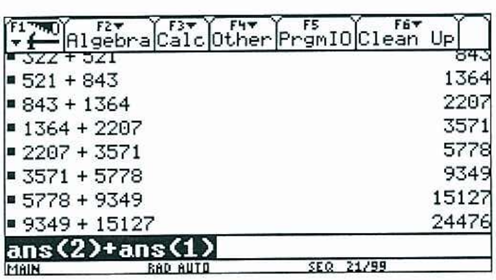


FIGURE 34 $(LUC(15)-LUC(21))$.

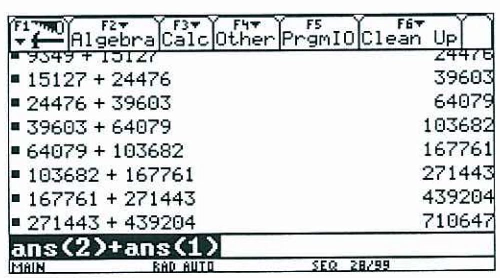


FIGURE 35 $(LUC(22)-LUC(28))$.

We next generate the first ten Lucas primes. See FIGURES 36-39 below:

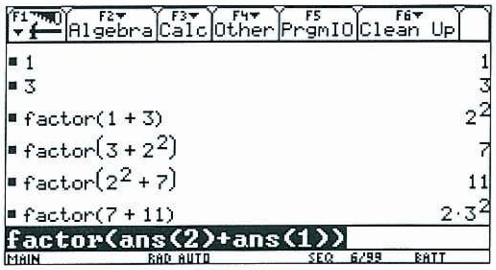


FIGURE 36 $(LUC(1)-LUC(7))$ factored.

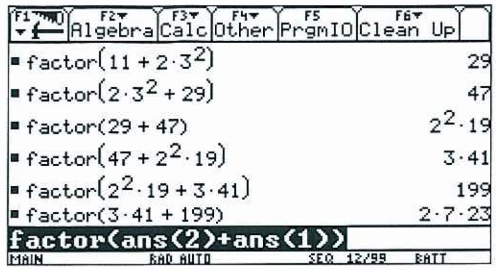


FIGURE 37 $(LUC(8)-LUC(14))$ factored.

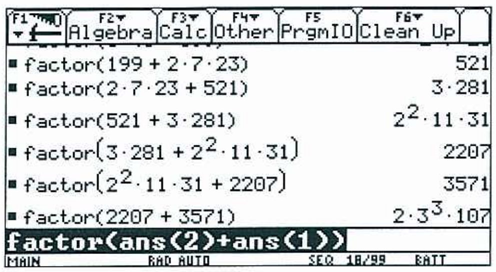


FIGURE 38 $(LUC(15)-LUC(21))$ factored.

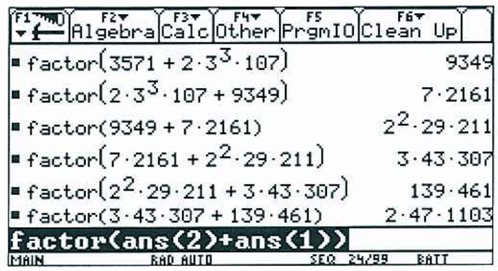


FIGURE 39 $(LUC(22)-LUC(28))$ factored.

Hence the first ten Lucas primes are as follows:

$$LUC(2)=3, LUC(4)=7, LUC(5)=11, LUC(7)=29, LUC(8)=47,$$
$$LUC(11)=199, LUC(13)=521, LUC(16)=2207, LUC(17)=3571, LUC(19)=9349.$$

Conclusion: Technology enables us to explore a world of possibilities. In this session, the role played by technology in three diverse number theoretic settings was addressed in the spirit of discovering exciting mathematical insights in conjunction with technology.