LARGE PROTH PRIMES WHEN $k = 21$ AND $k = 25$

Curtis Cooper
Department of Mathematics and Computer Science
Central Missouri State University
Warrensburg, MO 64093
cnc8851@cmsu2.cmsu.edu

1. Definitions and Theorems

<u>Definition 1</u>. A Proth prime is a prime number

$$N = k \cdot 2^n + 1,$$

where k is odd, n is a positive integer, and $0 < k < 2^n$.

They are named after the self taught farmer François Proth who lived near Verdun, France (1852-1879).

Proth Primes Less Than 2000

$$3 = 1 \cdot 2^1 + 1$$

$$5 = 1 \cdot 2^2 + 1$$

$$13 = 3 \cdot 2^2 + 1$$

$$17 = 1 \cdot 2^4 + 1$$

$$41 = 5 \cdot 2^3 + 1$$

$$97 = 3 \cdot 2^5 + 1$$

$$113 = 7 \cdot 2^4 + 1$$

$$193 = 3 \cdot 2^6 + 1$$

$$241 = 15 \cdot 2^4 + 1$$

$$257 = 1 \cdot 2^8 + 1$$

$$353 = 11 \cdot 2^5 + 1$$

$$449 = 7 \cdot 2^6 + 1$$

$$577 = 9 \cdot 2^6 + 1$$

$$641 = 5 \cdot 2^7 + 1$$

$$673 = 21 \cdot 2^5 + 1$$

$$769 = 3 \cdot 2^8 + 1$$

$$929 = 29 \cdot 2^5 + 1$$

$$1153 = 9 \cdot 2^7 + 1$$

$$1217 = 19 \cdot 2^6 + 1$$

$$1409 = 11 \cdot 2^7 + 1$$

$$1601 = 25 \cdot 2^6 + 1$$

Definition 2. The Fermat numbers are

$$F_n = 2^{2^n} + 1 \text{ for } n = 0, 1, 2, \ldots$$

and the Generalized Fermat numbers are

$$\mathrm{GF}(n, b) = b^{2^n} + 1,$$

where $n = 0, 1, 2, \ldots$ and $b > 1$ is an integer.

n	F_n
0	3
1	5
2	17
3	257
4	65537
5	$4294967297 = 641 \cdot 6700417$ (Euler)
6	$18446744073709551617 = 274177 \cdot 67280421310721$
7	340282366920938463463374607431768211457

For $0 \leq n \leq 4$, F_n is prime.

For $5 \leq n \leq 32$, F_n is composite.

The nature of F_{33} (prime or composite) is unknown.

The next theorem, attributed to Lucas, gives the nature of prime divisors of Fermat numbers. If k is small enough, these primes may be Proth.

Theorem 3. If $n > 1$ is a positive integer and p is a prime such that $p \mid F_n$, then p is of the form

$$p = k \cdot 2^{n+2} + 1,$$

where k is a positive integer.

Theorem 4 (Proth's Theorem). Let k be odd, $n \geq 2$, $0 < k < 2^n$ and $N = k \cdot 2^n + 1$ be a quadratic non-residue modulo a for some odd prime a. Then

$$N \text{ is prime}$$
$$\text{if and only if}$$
$$a^{(N-1)/2} \equiv -1 \pmod{N}.$$

2. VerticalProthSearch

VerticalProthSearch is a Yahoo group division of ProthSearch. This group was created to search for Proth primes from $k = 3$ to $k = 19$ and to provide a place for volunteers to reserve their ranges.

The ProthSearch web page is

http://www.prothsearch.net

The VerticalProthSearch web page is

http://proth.insider.com/vertical

"It appears that the probability of each prime of the form $k \cdot 2^n + 1$ dividing a Fermat number is $1/k$" (Harvey Dubner & Wilfrid Keller, "Factors of generalized Fermat numbers," *Mathematics of Computation,* Vol. 64, Number 209, January 1995, pp. 397–405.

k	Researcher	n Completed	n Reserved	T Sieved
3	Cosgrave	2,600,000	6,000,000	60
5	Toplic	1,530,000	1,656,000	
7	Nohara	1,130,000	2,000,000	15
9	Nohara	1,040,000	2,000,000	9
11	Eaton	750,000	1,500,000	
13	Grobstich			
15	Samidoost	700,000	1,000,000	
17	Grobstich			
19		700,000		
21	Cooper	1,160,000	2,000,000	0.8
23	Grobstich			
25	Cooper	1,060,000	1,360,000	0.35
27				
29	Nohara			
33	Keiser			
35	Keiser			
47	Nohara			

3. Nash Sieve and Proth Weight

Theorem 5. Let k be a fixed odd integer. For integers $x \geq 2$ and $0 \leq r < x$, let

$$g(x, r) = \gcd(2^x - 1, 2^r + k).$$

If $n \equiv -r \pmod{x}$, then $g(x, r)$ divides $k \cdot 2^n + 1$.

Proof. Assume $n \equiv -r \pmod{x}$. Then there exists a positive integer m such that $n + r = mx$. Therefore,

$$\begin{aligned} k \cdot 2^n &= k \cdot 2^{mx-r} \equiv -2^r 2^{mx-r} \pmod{g(x, r)} \\ &= -2^{mx} \pmod{g(x, r)} = -(2^x)^m \pmod{g(x, r)} \\ &= -(1)^m \pmod{g(x, r)} = -1 \pmod{g(x, r)}. \end{aligned}$$

Table of $g(x, r)$ for $k = 21$, $x \geq 2$, $0 \leq r < x$

$x \vert r$	0	1	2	3	4	5	6	7	8	9	10	11
2	1	1										
3	1	1	1									
4	1	1	5	1								
5	1	1	1	1	1							
6	1	1	1	1	1	1						
7	1	1	1	1	1	1	1					
8	1	1	5	1	1	1	85	1				
9	1	1	1	1	1	1	1	1	1			
10	11	1	1	1	1	1	1	1	1	1		
11	1	23	1	1	1	1	1	1	1	1	1	
12	1	1	5	1	1	1	5	1	1	13	5	1

Table of $g(x, r)$ for $k = 25$, $x \geq 2$, $0 \leq r < x$

$x \vert r$	0	1	2	3	4	5	6	7	8	9	10	11
2	1	3										
3	1	1	1									
4	1	3	1	3								
5	1	1	1	1	1							
6	1	9	1	3	1	3						
7	1	1	1	1	1	1	1					
8	1	3	1	3	1	3	1	51				
9	1	1	1	1	1	1	1	1	1			
10	1	3	1	33	1	3	1	3	1	3		
11	1	1	1	1	1	1	89	1	1	1	1	
12	13	9	1	3	1	3	1	9	1	3	1	3

Definition 6. The Proth weight for Proth primes with a fixed odd k is the number of unsieved values of n remaining over the range $1 \leq n < 10000$ after performing a Nash sieve with a (default) exponent limit of 256 and scaled by 1/1751.542. 1751.542 is something like an average weight.

Part of the reason for choosing $k = 21$ and $k = 25$ is because their Proth Weight's were 1.351380669 and 1.258319811, respectively. This compares to Proth Weight's for $k = 3$, $k = 5$, and $k = 7$ of 1.2172133175, 0.504698145, and 1.229202611, respectively. Another reason for choosing $k = 21$ and $k = 25$ is because they were the smallest k which were still available.

4. Procedure to Find Large Proth Primes When k Is Fixed

Step 1. Fix k and sieve primes up to some upper limit from the sequence $k \cdot 2^n + 1$ for $n = 1, 2, 3, \ldots$.

We sieved using Paul Jobling's NewPGen for Windows.

http://www.utm.edu/research/primes.programs/NewPGen/.

This program will maintain a file of numbers, k and n, which are not divisible by 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... (the primes up to a certain limit.)

The more sieving you can do the better.

The program's speed is dependent on the speed of your computer and its available memory.

For sieves of $k \cdot 2^n + 1$, the largest divisor candidate it can sieve is 1,152,921,504,606,846,976.

Ultimately, you want to sieve until the time it takes to throw out a k, n pair is about the time it takes to test the number $k \cdot 2^n + 1$ for primality. Actually, you may want to stop sieving just a little bit before this time. The rational here is that the ultimate goal is to find primes, not throw out composites.

Step 2. Run George Woltman's PRP program on the output from Paul Jobling's NewPGen program.

Woltman's program can be found at
http://sierpinski.insider.com/4847.

This will determine which of the numbers $k \cdot 2^n + 1$ are probably prime.

Step 3. If you obtain a probable prime $k \cdot 2^n + 1$ from Woltman's PRP program, test it on Yves Gallot's Proth program.

This program can be found at
http://www.utm.edu/research/primes/programs/gallot/.

It will prove whether or not your probable prime $k \cdot 2^n + 1$ is a prime. It will also test the number for divisibility of the Generalized Fermat numbers.

5. Results

http://www.prothsearch.net/riesel.html
List of Proth Primes For Specific k
March 24, 2005

Values of n When $k = 1$

1, 2, 4, 8, 16, [8589934591]

Values of n When $k = 3$

1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209,
276, 353, 408, 438, 534, 2208, 2816, 3168, 3189, 3912,
20909, 34350, 42294, 42665, 44685, 48150, 54792, 55182,
59973, 80190, 157169, 213321, 303093, 362765, 382449, [702000]
916773, 2145353, 2478785 g245

Values of n When $k = 5$

1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947, 3313,
4687, 5947, 13165, 23473, 26607, 125413, 209787, 240937,
819739, 1282755, 1320487 [1700000]

Values of n When $k = 7$

2, 4, 6, 14, 20, 26, 50, 52, 92, 120, 174, 180, 190, 290, 320, 390, 432, 616, 830, 1804, 2256, 6614, 13496, 15494, 16696, 22386, 54486, 88066, 95330, 207084, 283034, 561816, 804534, 811230, 1491852 [1500000]

Values of n When $k = 9$

1, 2, 3, 6, 7, 11, 14, 17, 33, 42, 43, 63, 65, 67, 81, 134, 162, 206, 211, 366, 663, 782, 1305, 1411, 1494, 2297, 2826, 3230, 3354, 3417, 3690, 4842, 5802, 6937, 7967, 9431, 13903, 22603, 24422, 39186, 43963, 47003, 49902, 67943, 114854, 127003, 145247, 147073, 149143, 304607, 384990, 412034, 435743, 461081 [720000] 834810 p148, 1051026 p156

Values of n When $k = 21$

1, 4, 5, 7, 9, 12, 16, 17, 41, 124, 128, 129, 187, 209, 276, 313, 397, 899, 1532, 1613, 1969, 2245, 2733, 4585, 4644, 6712, 6981, 13344, 17524, 27124, 29769, 47337, 55828, 91008, 94801, 164901, 179457, 191337, 200568, 220992 [420000] 686632, 856865, 1022168, 1240067, 1421741, 1830919 g279

Values of n When $k = 25$

2, 4, 6, 10, 20, 22, 52, 64, 78, 184, 232, 268,
340, 448, 554, 664, 740, 748, 1280, 1328, 1640,
3314, 3904, 3938, 5152, 9522, 57488, 66872, 148060,
154254, 216092 [230000] 302194 p144, 367294,
627710, 966414, 1211488, 1258562 g279

6. More Results

Chris Caldwell - University of Tennessee - Martin
http://www.utm.edu/staff/caldwell/
20 Largest Known Proth Primes
March 24, 2005

1. $28433 \cdot 2^{7830457} + 1$ 2357207 decimal digits SB7 2004

2. $5359 \cdot 2^{5054502} + 1$ 1521561 decimal digits SB6 2003

3. $3 \cdot 2^{2478785} + 1$ 746190 decimal digits g245 2003
   Divides F(2478782), GF(2478782,3),
   GF(2478776,6), GF(2478782,12)

4. $3 \cdot 2^{2145353} + 1$ 645817 decimal digits g245 2003
   Divides F(2145351), GF(2145351,3),
   GF(2145352,5), GF(2145348,6),
   GF(2145352,10), GF(2145351,12)

5. $21 \cdot 2^{1830919} + 1$ 551163 decimal digits g279 2004

6. $13 \cdot 2^{1499876} + 1$ 451509 decimal digits g267 2004
   Divides GF(1499875,3)

7. $7 \cdot 2^{1491852} + 1$ 449094 decimal digits p166 2005
Divides GF(1491851,6)

8. $21 \cdot 2^{1421741} + 1$ 427989 decimal digits g279 2005

9. $241489 \cdot 2^{1365062} + 1$ 410930 decimal digits L101 2005

10. $54767 \cdot 2^{1337287} + 1$ 402569 decimal digits SB5 2002

11. $5 \cdot 2^{1320487} + 1$ 397507 decimal digits g55 2002
Divides GF(1320486,12)

12. $5 \cdot 2^{1282755} + 1$ 386149 decimal digits g55 2002
Divides GF(1282754,3), GF(1282748,5)

13. $25 \cdot 2^{1258562} + 1$ 378867 decimal digits g279 2004
Generalized Fermat

14. $21 \cdot 2^{1240067} + 1$ 373299 decimal digits g279 2004

15. $25 \cdot 2^{1211488} + 1$ 364696 decimal digits g279 2005
Generalized Fermat, divides GF(1211487,12)

16. $69109 \cdot 2^{1157446} + 1$ 348431 decimal digits SB4 2002

17. $9 \cdot 2^{1051026} + 1$ 316392 decimal digits p156 2004
Generalized Fermat

18. $13 \cdot 2^{1038896} + 1$ 312740 decimal digits g267 2004

19. $21 \cdot 2^{1022168} + 1$ 307705 decimal digits g279 2004

20. $65567 \cdot 2^{1013803} + 1$ 305190 decimal digits SB2 2002

7. Future Work

1. Search for larger Proth primes When $k = 21$ and $k = 25$.

2. Find some new Proth primes Which Divide Fermat or Generalized Fermat Numbers.