MATHEMATICS OF COMPUTATION
Volume 76, Number 260, October 2007, Pages 2087–2094
S 0025-5718(07)01955-2
Article electronically published on April 17, 2007

A SEARCH FOR FIBONACCI-WIEFERICH AND WOLSTENHOLME PRIMES

RICHARD J. MCINTOSH AND ERIC L. ROETTGER

ABSTRACT. A prime p is called a *Fibonacci-Wieferich prime* if $F_{p-(\frac{p}{5})} \equiv 0 \pmod{p^2}$, where F_n is the nth Fibonacci number. We report that there exist no such primes $p < 2 \times 10^{14}$. A prime p is called a *Wolstenholme prime* if $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$. To date the only known Wolstenholme primes are 16843 and 2124679. We report that there exist no new Wolstenholme primes $p < 10^9$. Wolstenholme, in 1862, proved that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ for all primes $p \geq 5$. It is estimated by a heuristic argument that the "probability" that p is Fibonacci-Wieferich (independently: that p is Wolstenholme) is about $1/p$. We provide some statistical data relevant to occurrences of small values of the Fibonacci-Wieferich quotient $F_{p-(\frac{p}{5})}/p$ modulo p.

1. INTRODUCTION

Let P and Q be nonzero integers. The Lucas sequences $\{U_n\} = \{U_n(P,Q)\}$ and $\{V_n\} = \{V_n(P,Q)\}$ associated to the pair (P,Q) are defined by

$$U_0 = 0\,,\ U_1 = 1\,,\ U_{n+1} = PU_n - QU_{n-1} \ \text{ for } \ n \geq 1\,,$$

and

$$V_0 = 2\,,\ V_1 = P\,,\ V_{n+1} = PV_n - QV_{n-1} \ \text{ for } \ n \geq 1\,.$$

The discriminant of the characteristic polynomial of these sequences is given by $D = P^2 - 4Q$. We will assume that $D \neq 0$. The special case $P = -Q = 1$ defines the well-known Fibonacci sequence, which we will denote by $\{F_n\} = \{U_n(1,-1)\}$, and the Lucas numbers usually denoted by $\{L_n\} = \{V_n(1,-1)\}$.

It is well-known (see [5, pp. 393–395]) that $F_{p-(\frac{p}{5})}$ is divisible by p, where p is prime and $(\frac{p}{5})$ denotes the Legendre symbol. If $F_{p-(\frac{p}{5})}$ is divisible by p^2, then we call p a *Fibonacci-Wieferich prime* (these primes are sometimes called Wall-Sun-Sun primes [3, pp. 110–112]). A *Wieferich prime* is a prime p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$.

According to the most recent search [9] the only Wieferich primes $p < 1.25 \times 10^{15}$ are 1093 and 3511. Williams [19] found no Fibonacci-Wieferich primes below 10^9 and Montgomery [11] extended this to 2^{32}. Our computer search found no such primes below 2×10^{14}. Of historical interest is the connection between Fibonacci-Wieferich primes and Fermat's Last Theorem. Sun and Sun [17] proved that if

Received by the editor June 14, 2005 and, in revised form, May 19, 2006.
2000 *Mathematics Subject Classification.* Primary 11A07, 11A41, 11B39, 11Y99.
Key words and phrases. Fibonacci number, Wieferich prime, Wall-Sun-Sun prime, Wolstenholme prime.

the first case of Fermat's Last Theorem fails for the exponent p, then p must be a Fibonacci-Wieferich prime.

2. Lucas-Wieferich primes

Returning to the general Lucas Sequences $\{U_n(P,Q)\}$ and $\{V_n(P,Q)\}$, we have $U_{p-(\frac{D}{p})}$ divisible by p whenever p is a prime not dividing $2Q$. Let ϵ denote the Legendre symbol $(\frac{D}{p})$, where $D = P^2 - 4Q$. The modulo p residues of $U_{p-\epsilon}$, $V_{p-\epsilon}$, U_p and V_p are given by the following congruences, valid for primes p not dividing $2QD$:

$$U_{p-\epsilon} \equiv 0 \pmod{p}, \tag{1}$$

$$V_{p-\epsilon} \equiv 2Q^{(1-\epsilon)/2} \pmod{p}, \tag{2}$$

$$U_p \equiv \epsilon \pmod{p}, \tag{3}$$

$$V_p \equiv P \pmod{p}. \tag{4}$$

For a detailed discussion of these and many other congruences for Lucas sequences we refer the reader to Ribenboim [14] and Riesel [15].

Congruence (2) enjoys the following (mod p^2) extension.

Lemma. *If the prime p does not divide $2QD$, then*

$$V_{p-\epsilon} \equiv Q^{(1-\epsilon)/2}(Q^{p-1}+1) \pmod{p^2}. \tag{5}$$

Proof. We begin with equations (IV.4) with $n = m$ and (IV.5) in [14, p. 57]:

$$2V_{2m} = V_m^2 + DU_m^2 \tag{6}$$

and

$$V_{2m} = V_m^2 - 2Q^m. \tag{7}$$

Subtracting (7) from (6) yields

$$V_{2m} = DU_m^2 + 2Q^m. \tag{8}$$

Let $2m = p - \epsilon$ and $\mu = (\frac{Q}{p})$ denote the Legendre symbol. By [14, p. 63], statement (IV.23), we have $p|U_m$ if $\mu = 1$ and $p|V_m$ if $\mu = -1$. Therefore, it follows from (8) if $\mu = 1$ and from (7) if $\mu = -1$ that

$$V_{p-\epsilon} = V_{2m} \equiv 2\mu Q^m = 2\mu Q^{(p-\epsilon)/2} = 2\mu Q^{(p-1)/2}Q^{(1-\epsilon)/2} \pmod{p^2}. \tag{9}$$

Since $Q^{(p-1)/2} \equiv \mu \pmod{p}$ by Euler's criterion, we have $Q^{(p-1)/2} \equiv \mu(1+ap) \pmod{p^2}$ for some integer a. Hence $Q^{p-1} \equiv 1 + 2ap \pmod{p^2}$, and therefore $2\mu Q^{(p-1)/2} \equiv 2 + 2ap \equiv Q^{p-1} + 1 \pmod{p^2}$. Finally, by (9) we obtain $V_{p-\epsilon} \equiv (Q^{p-1}+1)Q^{(1-\epsilon)/2} \pmod{p^2}$, which completes the proof of (5).

Sometimes $U_{p-\epsilon}$ is divisible by p^2. We call these primes *Lucas-Wieferich primes* associated to the pair (P,Q). Every Wieferich prime is a Lucas-Wieferich prime associated to the pair $(3,2)$. Equivalent congruences for Lucas-Wieferich primes are given in Theorem 1.

Theorem 1. *If the prime p does not divide $2PQD$, then the following are equivalent*:

(i) $U_{p-\epsilon} \equiv 0 \pmod{p^2}$,
(ii) $V_{p-\epsilon} \equiv 2\mu Q^{(p-\epsilon)/2} \pmod{p^4}$,

(iii) $V_{p-\epsilon} \equiv 2\mu Q^{(p-\epsilon)/2} \pmod{p^3}$,
(iv) $U_p \equiv \epsilon(Q^{p-1}+1)/2 \pmod{p^2}$,
(v) $V_p \equiv P(Q^{p-1}+1)/2 \pmod{p^2}$.

Proof. We will first show that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii). Suppose that $U_{p-\epsilon} \equiv 0 \pmod{p^2}$. By [14, p. 56], equation (IV.1), we have $V_{p-\epsilon}^2 - 4Q^{p-\epsilon} = DU_{p-\epsilon}^2$. Hence $(V_{p-\epsilon} - 2\mu Q^{(p-\epsilon)/2})(V_{p-\epsilon} + 2\mu Q^{(p-\epsilon)/2}) = V_{p-\epsilon}^2 - 4Q^{p-\epsilon} = DU_{p-\epsilon}^2 \equiv 0 \pmod{p^4}$, where $\mu = (\frac{Q}{p})$ denotes the Legendre symbol. By (9) we have $V_{p-\epsilon} - 2\mu Q^{(p-\epsilon)/2} \equiv 0 \pmod{p}$, which implies that $V_{p-\epsilon} + 2\mu Q^{(p-\epsilon)/2} \not\equiv 0 \pmod{p}$ since p does not divide $2Q$. Therefore $V_{p-\epsilon} - 2\mu Q^{(p-\epsilon)/2} \equiv 0 \pmod{p^4}$, and so $V_{p-\epsilon} \equiv 2\mu Q^{(p-\epsilon)/2} \pmod{p^4}$.

(ii) $\Rightarrow$ (iii) is trivial.

(iii) $\Rightarrow$ (i). Suppose that $V_{p-\epsilon} \equiv 2\mu Q^{(p-\epsilon)/2} \pmod{p^3}$. Then $V_{p-\epsilon}^2 - 4Q^{p-\epsilon} = (V_{p-\epsilon} - 2\mu Q^{(p-\epsilon)/2})(V_{p-\epsilon} + 2\mu Q^{(p-\epsilon)/2}) \equiv 0 \pmod{p^3}$ and so by [14, p. 56], equation (IV.1), it follows that $DU_{p-\epsilon}^2 = V_{p-\epsilon}^2 - 4Q^{p-\epsilon} \equiv 0 \pmod{p^3}$. Since p does not divide D we obtain (i).

Next, we will prove that (i) and (iv) are equivalent. By [14, p. 56], equation (IV.2), we have $V_n = U_{n+1} - QU_{n-1}$. Using the recurrence $U_{n+1} = PU_n - QU_{n-1}$ we obtain

$$V_n = 2U_{n+1} - PU_n \tag{10}$$

and

$$V_n = PU_n - 2QU_{n-1}\,. \tag{11}$$

Setting $n = p-1$ in (10) and $n = p+1$ in (11) we get

$$V_{p-1} = 2U_p - PU_{p-1} \tag{12}$$

and

$$V_{p+1} = PU_{p+1} - 2QU_p\,. \tag{13}$$

Using (12) when $\epsilon = 1$ and (13) when $\epsilon = -1$ we obtain

$$V_{p-\epsilon} = -\epsilon PU_{p-\epsilon} + 2\epsilon Q^{(1-\epsilon)/2}U_p\,.$$

By (5) we have $V_{p-\epsilon} \equiv Q^{(1-\epsilon)/2}(Q^{p-1}+1) \pmod{p^2}$. Therefore

$$2Q^{(1-\epsilon)/2}U_p - PU_{p-\epsilon} \equiv \epsilon Q^{(1-\epsilon)/2}(Q^{p-1}+1) \pmod{p^2}\,.$$

Since p does not divide $2PQ$ the equivalence of (i) and (iv) follows from the above congruence.

Finally, we will prove that (i) and (v) are equivalent. By [14, p. 56], equation (IV.2), we have $DU_n = V_{n+1} - QV_{n-1}$. Using the recurrence $V_{n+1} = PV_n - QV_{n-1}$ we obtain

$$DU_n = 2V_{n+1} - PV_n \tag{14}$$

and

$$DU_n = PV_n - 2QV_{n-1}\,. \tag{15}$$

Setting $n = p-1$ in (14) and $n = p+1$ in (15) we get

$$DU_{p-1} = 2V_p - PV_{p-1} \tag{16}$$

and

$$DU_{p+1} = PV_{p+1} - 2QV_p\,. \tag{17}$$

Using (16) when $\epsilon = 1$ and (17) when $\epsilon = -1$ we obtain

$$DU_{p-\epsilon} = -\epsilon PV_{p-\epsilon} + 2\epsilon Q^{(1-\epsilon)/2}V_p\,.$$

By (5) we have $V_{p-\epsilon} \equiv Q^{(1-\epsilon)/2}(Q^{p-1}+1) \pmod{p^2}$. Therefore

$$2Q^{(1-\epsilon)/2}V_p - \epsilon DU_{p-\epsilon} \equiv PQ^{(1-\epsilon)/2}(Q^{p-1}+1) \pmod{p^2}\,.$$

Since p does not divide $2QD$ the equivalence of (i) and (v) follows from the above congruence. The proof of Theorem 1 is now complete. □

Sun [16] showed that p is a Fibonacci-Wieferich prime if and only if $L_{p-\epsilon} \equiv 2\epsilon \pmod{p^4}$, which proves that (i) and (ii) are equivalent when $P = -Q = 1$.

3. Algorithm for the Fibonacci-Wieferich prime search

In general there is no known way to resolve $F_{p-(\frac{p}{5})} \pmod{p^2}$, other than through explicit computations. From the recurrence $F_{n+1} = F_n + F_{n-1}$ we obtain

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Powers of the above matrix are computed (mod p^2) by a standard binary power ladder. Since our 64-bit processors cannot handle products of magnitude p^4, we invoked base p representations and thereby "split" the multiplication of two numbers (mod p^2). Every $x = a + bp \pmod{p^2}$ is represented by $\{a, b\}$, with both a, b always reduced (mod p). To avoid repeated use of long division by p we computed and stored the value of $1/p$ in double precision floating-point. The quotient k/p is given by $\lfloor 0.5 + k(1/p) \rfloor$ and the remainder is given by $k - \lfloor 0.5 + k(1/p) \rfloor$. If the remainder is negative, then p is added to the remainder and 1 is subtracted from the quotient. Crandall [3, pp. 9–10] calls this "steady-state division". Overflow errors do not occur when $p < 4 \times 10^{14}$ and $k < p^2$. The final value of $F_{p-(\frac{p}{5})} \equiv B + Ap \pmod{p^2}$ is represented by $\{B, A\}$, where $0 \le B < p$ and $-p/2 < A < p/2$. If $B \neq 0$, our program exits with fatal error. Instances of $|A| \le 100$ are recorded (see Table 1 below) for testing purposes and statistical analysis. The value $A = 0$ would signify a Fibonacci-Wieferich prime. Extremely close calls ($A = \pm 1$) occur when $p = 2$, 3, 5, 17, 251, 733, 1063, 123863 and 1677209.

We were interested in applying the above test only to actual primes p. Due to the nature of binary power ladder we found it wasteful to employ the Fermat test, that is, whether $2^{p-1} \equiv 1 \pmod{p}$, for selecting primes. Instead we used an incremental sieve designed by Crandall [3, p. 100] which sieves the integers in blocks of a million at a time.

Most of the computation was performed on an SGI Onyx/2 server with 24 R12000 processors and 12 GB of RAM, running IRIX 6.5. Near the end of the search range each processor was capable of processing an interval of 45×10^9 integers per day or about 16000 primes per second. About 10% of the total running time was used for sieving the primes. Taking advantage of 64-bit processors our program was about 7 times faster than the program used in [9] which was designed for 32-bit processors.

TABLE 1. Instances of $F_{p-(\frac{p}{5})} \equiv Ap \pmod{p^2}$ with $|A| \leq 100$ and $2^{32} < p < 2 \times 10^{14}$

p	A
6627557731	−43
6741860329	80
6859114489	55
8352762221	94
9760159421	−30
10115341939	70
10536116749	66
10612008943	−69
11002117921	95
11025166637	23
12216759923	−33
12387724249	39
13585864301	57
13699540891	73
13941800291	15
16368086681	50
16548311011	92
17370126353	−70
18526398173	−29
20488487861	−92
24178397183	3
25049632411	51
31811337589	−89
37883499127	−10
50261755937	−73
65543096747	−36
74176637257	−70
82202291813	−11
87918267869	78

p	A
89845144679	51
94903475011	−15
101876918491	87
110717352637	−77
111646394549	−86
115301883659	60
115364673283	62
129316722167	−22
134431860461	−30
166466703223	64
170273590301	78
233642484991	89
277764184829	64
283750593739	37
300258464153	70
334015396151	79
442650398821	74
458432241569	−61
621291852133	96
762383958397	−86
766193665711	−8
800537116979	−20
1082150673011	−57
1171853196853	−30
1551559563569	4
1786416720937	−82
1996100161327	98
2669682790919	−10
3311519272973	−47

p	A
3814438808399	−56
3858738583171	44
5457214172491	76
8030311150847	−12
10591568377751	33
11406840440243	26
11456600879363	−41
12801531958729	17
13860200708287	−5
18801391545961	33
21960966892313	54
22548139284371	−16
25186595067349	−59
26861987497291	−28
28263796914043	−88
39568597208207	53
46006966741789	−59
64241561031937	−44
67721845179979	−52
75320741942123	71
82789107950701	−42
85136199318719	−92
86040142362653	19
88536418898561	99
90299689540433	56
91486955300761	−71
106692167197171	−85
155979357644989	27

4. Statistical considerations

Are there any Fibonacci-Wieferich primes? Since $A = A(p)$ is an integer in the interval $(-p/2, p/2)$, one might assume that the "probability" of A taking on any particular value, say the value 0, is equal to $1/p$. One might view the Fibonacci-Wieferich test for different primes as "independent" events. Therefore, by this heuristic argument the number of Fibonacci-Wieferich primes in an interval $[x, y]$ is expected to be

$$\sum_{x \leq p \leq y} \frac{1}{p} \approx \sum_{n=x}^{y} \frac{1}{n \ln n} \approx \int_x^y \frac{dt}{t \ln t} = \ln(\ln y) - \ln(\ln x),$$

since it follows from the Prime Number Theorem that the "probability" that an integer p is prime is about $1/\ln p$. If this is the case, then the expected number of Fibonacci-Wieferich primes in the interval $[2^{32}, 2 \times 10^{14}]$ is approximately 0.395,

and so there was indeed a fairly good chance to find a Fibonacci-Wieferich prime, which justifies the effort in undertaking this search.

If we take into account "near" Fibonacci-Wieferich primes, that is, primes p with $|A| \le 100$, then the expected number of "close calls" in the above interval is approximately $201 \times 0.395 \approx 79.4$. From Table 1 we see that the actual count is 86.

5. Wolstenholme primes

In 1862 Wolstenholme [20] (also see [5, p. 271] and [14, p. 29]) proved that $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$ for all primes $n \ge 5$. McIntosh [10] found no composite solutions $n < 10^9$, and it is conjectured that there are none [7, problem B31]. Unlike that of Wilson's Theorem the converse of Wolstenholme's Theorem is a very difficult problem.

The term *Wolstenholme prime* has been introduced in [10] for primes p satisfying the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$. In [10, p. 386] the following theorem was proved, where B_n denotes the nth Bernoulli number.

Theorem 2. *For all primes $p \ge 11$ the following are equivalent*:

(i) *p is a Wolstenholme prime,*

(ii) *p divides the numerator of B_{p-3},*

(iii) $\sum_{p/6<k<p/4} \frac{1}{k^3} \equiv 0 \pmod{p}$.

Statement (ii) appears in a criterion concerning Fermat's Last Theorem. A prime p is *regular* if and only if p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. For all such primes the algebraic proof of Fermat's Last Theorem is valid (see [6, p. 244] and [13, p. 10]). This was one of the main reasons for the search of irregular primes. Buhler, Crandall, Ernvall, and Metsänkylä [1] calculated all irregular primes up to 4×10^6 by evaluating sums of like powers of numbers in arithmetic progression, and these calculations were extended in [2] by use of different methods to 12×10^6.

The Wolstenholme primes are those irregular primes where p divides the numerator of B_{p-3}. The only known Wolstenholme primes are 16843 and 2124679. The first was found (though not explicitly reported) by Selfridge and Pollak (Notices AMS **11** (1964), 97), and later confirmed by W. Johnson [8] and S.S. Wagstaff (Notices AMS **23** (1976), A-53). The second was found by J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä [1], and later, independently, by McIntosh [10, p. 387] in his search up to 2×10^8. Using (iii) we extended the search to 10^9 and found no new Wolstenholme primes, and thus no new primes p divide the numerator of B_{p-3}.

Our program, written by Montgomery [12], evaluates the least two significant coefficients c_0 and $c_1 \pmod{p}$ in the polynomial

$$f(x) = \prod_{p/6<k<p/4} (x + k^3)$$

by the use of a polynomial scheme similar to the one developed in [4, p. 441]. The sum $(\mathrm{mod}\ p)$ of the reciprocals of the roots of $f(x)$ is given by $-c_1/c_0$. The value $c_1 = 0$ would signify a Wolstenholme prime. The fast Fourier transform (FFT) and the Nussbaumer convolution were not used. Most of the computation was performed on an SGI Onyx/2 server with 24 R12000 processors and 12 GB

of RAM, running IRIX 6.5. Near the end of the search range each processor was capable of processing an interval of 412000 integers per day or about 4.3 seconds per prime. The Fermat test, that is, whether $2^{p-1} \equiv 1 \pmod{p}$, was used for selecting primes. Due to the relatively long time required to process each prime the use of a sieve for selecting primes would not offer a significant reduction in total running time.

Acknowledgments

The authors are grateful to Richard Crandall, Joshua Knauer and Peter Montgomery for their help in the search for Fibonacci-Wieferich and Wolstenholme primes. Support by the Natural Sciences and Engineering Research Council of Canada is gratefully acknowledged.

References

[1] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, *Math. Comp* **61** (1993) 151–153. MR1197511 (93k:11014)

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M.A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comput* **31** (2001) 89–96. MR1806208 (2001m:11220)

[3] R.E. Crandall, *Topics in Advanced Scientific Computation*, TELOS/Springer-Verlag, Santa Clara, CA, 1996. MR1392472 (97g:65005)

[4] R.E. Crandall, K. Dilcher, and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp* **66** (1997) 433–449. MR1372002 (97c:11004)

[5] L.E. Dickson, *The History of the Theory of Numbers*, vol. 1, Reprinted: Chelsea Publishing Company, New York, 1966.

[6] H.M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, New York, 1977. MR616635 (83b:12001a)

[7] R.K. Guy, *Unsolved Problems in Number Theory*, Third ed., Springer-Verlag, New York, 2004. MR2076335 (2005h:11003)

[8] W. Johnson, Irregular primes and cyclotomic invariants, *Math. Comp* **29** (1975) 113–120. MR0376606 (51:12781)

[9] J. Knauer and J. Richstein, The continuing search for Wieferich primes, *Math. Comp* **74** (2005) 1559–1563. MR2137018 (2006a:11006)

[10] R.J. McIntosh, On the converse of Wolstenholme's Theorem, *Acta Arith* **71** (1995) 381–389. MR1339137 (96h:11002)

[11] P. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp* **61** (1991) 361–363. MR1182246 (94d:11003)

[12] ———, private communication, 1993.

[13] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979. MR551363 (81f:10023)

[14] ———, *The New Book of Prime Number Records*, Third ed., Springer-Verlag, New York, 1996. MR1377060 (96k:11112)

[15] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser Publishers, Boston, 1985. MR897531 (88k:11002)

[16] Z.-H. Sun, private communication, 2005.

[17] Z.-H. Sun and Z.-W. Sun, Fibonacci numbers and Fermat's last theorem, *Acta Arith* **60** (1992) 371–388. MR1159353 (93e:11025)

[18] D.D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532. MR0120188 (22:10945)

[19] H.C. Williams, The influence of computers in the development of number theory, *Comput. Math. Appl* **8** (1982) 75–93. MR649653 (83c:10002)

[20] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Math* **5** (1862) 35–39.

Department of Mathematics and Statistics, University of Regina, Regina, Saskatchewan, Canada S4S 0A2
E-mail address: mcintosh@math.uregina.ca

Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada T2N 1N4
E-mail address: roettgee@math.ucalgary.ca