TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 306, Number 1, March 1988

THE FIRST CASE OF FERMAT'S LAST THEOREM IS TRUE FOR ALL PRIME EXPONENTS UP TO 714,591,416,091,389

ANDREW GRANVILLE AND MICHAEL B. MONAGAN

ABSTRACT. We show that if the first case of Fermat's Last Theorem is false for prime exponent p then p^2 divides $q^p - q$ for all primes $q \leq 8q$. As a corollary we state the theorem of the title.

1. The history of FLT. In about 1637, Fermat asserted, in the margin of his copy of the complete works of Diophantus, that it is not possible to find, for a given integer $n > 2$, nonzero integers x, y and z such that

$$(1)_n \qquad x^n + y^n = z^n.$$

Fermat himself established the above for exponent $n = 4$. It is clear that, in order to prove Fermat's assertion, it suffices to prove that $(1)_p$ has no solutions for all prime exponents $p \geq 3$, and under the assumption that x, y and z are pairwise coprime.

It is traditional to split Fermat's Last Theorem into two cases:

(I) where exponent p does not divide xyz;

(II) where exponent p does divide xyz.

In this paper we shall be examining the First Case of Fermat's Last Theorem for prime exponent p, $(\text{FLTI})_p$; that is the assertion that

There do not exist nonzero, pairwise relatively prime integers x, y and z such that

$$(2)_p \qquad x^p + y^p + z^p = 0 \quad \text{and} \quad p \text{ does not divide } xyz.$$

The first attempt to prove $(\text{FLTI})_p$ for a class of prime exponents was made by Sophie Germain, in 1823, who showed that if p and $2p + 1$ are both primes then $(\text{FLTI})_p$ is true. Legendre [**14**] extended this result to $4p+1$, $8p+1$, $10p+1$, $14p+1$ and $16p + 1$ and showed as a corollary that $(\text{FLTI})_p$ holds for all primes $p < 100$.

In 1894, Wendt [**34**] extended Sophie Germain's Theorem to prove that $(\text{FLTI})_p$ holds for prime p, if there exists an even integer m, not divisible by 3, such that p does not divide $m^m - 1$, $q = mp + 1$ is prime and q does not divide $N_m = \prod_{\xi^m=1}[(1+\xi)^m - 1]$. Dickson [**5**] made extensive computations of the prime factors of $m^m - 1$ and N_m to prove $(\text{FLTI})_p$ for all $p < 7000$.

In 1847 Kummer [**12**] showed that Fermat's Last Theorem holds for exponent p whenever p is a 'regular' prime—i.e. p does not divide B_{2n} for any $2 \leq 2n \leq p - 3$,

Received by the editors December 2, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41; Secondary 11B68, 15A15, 68K99.

This work was partially supported by NSERC of Canada under operating grant numbers A0894, A3353, G1587, 126-6027, 126-6028, 126-6101, 126-6445.

©1988 American Mathematical Society
0002-9947/88 $1.00 + $.25 per page

where B_n is the nth Bernoulli number; that is

$$\frac{X}{e^X - 1} = \sum_{n \geq 0} B_n \frac{X^n}{n!}.$$

In 1976, Wagstaff [**33**] used Kummer's criterion to prove Fermat's Last Theorem for all exponents up to 125,000. However, due to the difficulty of computing $B_n \pmod p$, it seems unlikely that this method will lead to any significant increase on 125,000. Tanner and Wagstaff (Math. Comp. **48** (1987), 341–350) have extended these computations to 150,000.

Throughout we shall take x, y, z to be a solution of $(2)_p$. Let $G = G_{[x,y,z]}$ be the set of congruence classes $(\mathrm{mod}\, p)$ of $-x/y$, $-x/z$, $-y/x$, $-y/z$, $-z/x$ and $-z/y$. Note that 0 and 1 are not elements of G as p does not divide xyz. As $x+y+z \equiv 0 \pmod p$, we also note that if $t \in G$ then G is precisely the set of congruence classes of $t, 1-t, 1/t, 1/(1-t)$, $t/(t-1)$ and $1-1/t \pmod p$.

In 1857 Kummer [**13**] considered the first case in far greater detail. Let

$$\frac{1}{1 - te^X} = \sum_{n \geq 0} f_n(t) \frac{X^n}{n!}.$$

Kummer proved

LEMMA 1. *If* $t \in G_{[x,y,z]}$ *then* $B_{p-1-n} f_n(t) \equiv 0 \pmod p$ *for* $n = 1, 2, \ldots, p-2$.

In 1905, Mirimanoff [**20**] proved

LEMMA 2. *If* $t \in G_{[x,y,z]}$ *then* $f_n(t) f_{p-2-n}(t) \equiv 0 \pmod p$ *for* $n = 0, 1, 2, \ldots, p-2$.

In 1925, Vandiver [**31**, Corollary I] extended this to

LEMMA 3. *If* $t, u \in G_{[x,y,z]}$ *then* $f_n(t) f_{p-2-n}(u) \equiv 0 \pmod p$ *for* $n = 0, 1, 2, \ldots, p-2$.

In 1909, Wieferich [**35**] produced the following astounding result.

LEMMA 4. *If* $(\mathrm{FLTI})_p$ *is false for prime* p *then* p^2 *divides* $2^p - 2$.

Extensive computations by D. H. Lehmer [**15**], in 1981, showed that p^2 divides $2^p - 2$ only for primes $p = 1093$ and 3511 where $p < 6.10^9$; and, as a corollary proved that $(\mathrm{FLTI})_p$ is true for all primes $p < 6.10^9$.

In 1910, Mirimanoff [**21**] extended Wieferich's result by showing that if $(\mathrm{FLTI})_p$ is false for prime p then p^2 divides $3^p - 3$ (N.B. p^2 does not divide $3^p - 3$ for $p = 1093$ and 3511).

In this paper we shall use an induction hypothesis to show that if $(\mathrm{FLTI})_p$ is false for prime p then p^2 divides $q^p - q$ for each successive prime q up to 89. This technique was first used by Frobenius [**7**] in 1914; however Frobenius was unsuccessful in applying the technique.

In 1917, Pollaczek [**24**], using a similar method, claimed to have proved that if $(\mathrm{FLTI})_p$ is false then p^2 divides $q^p - q$ for all primes $q \leq 31$. However, in his paper, Pollaczek only proved the result for p sufficiently large ($p > \alpha^{q^2/3}$ where $\alpha = (\sqrt{5}+1)/2$). A number of other minor errors appear in his paper.

In 1931, Morishima [**22**] claimed to have extended the result to all primes $q \leq 43$, applying the method of Frobenius. However Gunderson [**10**], in his doctoral thesis, raised objections to a number of the proofs in Morishima's paper. Despite Morishima's claims to the contrary, Gunderson's objections are for the most part valid, and he succeeded in repairing a number of the proofs. We do have a number of further objections to Morishima's paper. For instance, he proves (quite vaguely) the assertion up to $q = 31$ and then states that one does the calculations up to $q = 43$, "*In analoger Weise*"! We shall see that there are such large computational difficulties in the gap from 31 to 43 that we cannot really accept this as valid mathematical proof.

In 1941, Lehmer and Lehmer [**16**] considered primes p for which it would be possible that $q^p \equiv q \pmod{p^2}$ for each prime $q \leq 43$. Using a method of counting lattice points in 14-dimensional space they showed that $p > 253,747,889$. In 1948, their method was superceded by one of Gunderson [**10**]. He showed

LEMMA 5. *Let $\{q_1, q_2, q_3, \ldots, q_n\}$ be a set of primes and suppose that p is a prime such that p^2 divides $q_i^p - q_i$ for each $i = 1, \ldots, n$. Then*

$$g_n(p) = 4\binom{2n-2}{n-1}\frac{[\log(p/\sqrt{2})]^n}{n!\log q_1 \log q_2 \cdots \log q_n} \leq p - 1.$$

As $q^p \equiv q \pmod{p^2}$ for each prime $q \leq 31$, whenever $(\mathrm{FLTI})_p$ is false for prime p, Gunderson showed that $(\mathrm{FLTI})_p$ holds for each prime $p \leq 1,110,601,027$.

In 1981, Shanks and Williams [**30**] examined Gunderson's function $g_n(p)$ in detail and showed that $g_n(p) \leq p - 1$ for all $n \geq 30$ and $p > 4.2 \times 10^{15}$. In other words, Lemma 5 is of no interest for $n \geq 30$.

However, Shanks and Williams observed that if one could show that $(\mathrm{FLTI})_p$ is false implies p^2 divides $q^p - q$ for each $q \leq 109$ then $(\mathrm{FLTI})_p$ is true for $p \leq 4,408,660,978,137,503$. Although this was our initial objective, we were only able to complete the computations as far as $q = 89$, and so prove the theorem stated in the title. These computations were done using the Maple system on DEC VAX machines at the University of Waterloo.

We will also show that if a specific class of matrices in $\mathbf{Z}[X]$ have certain properties (see Conjecture 3), and if $(\mathrm{FLTI})_p$ is false then p^2 divides $q^p - q$ for each prime $q \leq 3 + 1.643(\log p)^{1/4}$. In a forthcoming paper the first author will prove that for each prime $p \geq 5$ there exists a prime $q < (\log p)^2$ for which $p^2 \nmid q^p - q$. This would imply that a proof of Conjecture 3 would be the first step on the road to a proof of (FLTI)!

Finally we note that $(\mathrm{FLTI})_p$ has recently been shown to be true for infinitely many distinct prime exponents p by Adleman and Heath-Brown [**1**], using Fouvry's remarkable work on the Brun-Titchmarsh inequality [**6**], and Wendt's extension of Sophie Germain's Theorem.

Before starting on our exposition we will point out the main difference in our approach to that of Frobenius, Pollaczek, Morishima and Gunderson. The power series $1/(1-te^X)$ is central to our investigations (in an examination of Hasse's work [**11**] it is clear that this follows naturally from considerations of the Hilbert norm residue symbol). Certain other power series of the form $e^{iX}/(1-te^{kX})$ also appear. In our approach we establish a number of identities involving these power series and only consider the value of $f_n(t) \pmod{p}$ later on. In the classical approach,

stemming from an observation of Mirimanoff, the polynomials $f_n(t)$ are evaluated (mod p) at a very early stage. This has made most of the proofs very difficult to follow, and has led to many of the errors that have appeared. A pleasant way to understand the observation of Mirimanoff is as follows:

$$\sum_{n\geq 0} f_n(t)\frac{X^n}{n!} = \frac{1}{1-te^X} = \left(\sum_{j=0}^{p-1} t^j e^{jX}\right) \Big/ \left(1-t^p e^{pX}\right)$$

$$= \left(\sum_{n\geq 0}\left(\sum_{j=0}^{p-1} j^n t^j\right)\frac{X^n}{n!}\right)\left(\sum_{n\geq 0} p^n f_n(t^p)\frac{X^n}{n!}\right).$$

But then if $t \not\equiv 0$ or $1 \pmod p$, we see that

$$f_n(t) \equiv \left(\sum_{j=0}^{p-1} j^n t^j\right) \Big/ (1-t^p) \pmod p.$$

These previous authors have substituted $\sum_{j=0}^{p-1} j^n t^j$ in place of $f_n(t)$ in their computations; and this has often led to quite severe complications.

We note here that by the above approach:

LEMMA 6. *If $t \not\equiv 0$ or $1 \pmod p$ then $f_{p-1}(t) \equiv 0 \pmod p$.*

PROOF.

$$f_{p-1}(t) \equiv \left(\sum_{j=0}^{p-1} j^{p-1} t^j\right) \Big/ (1-t^p)$$

$$\equiv \left(\sum_{j=1}^{p-1} t^j\right) \Big/ (1-t) \equiv \frac{t-t^p}{(1-t)^2} \equiv 0 \pmod p.$$

2. The Kummer-Mirimanoff criteria. Throughout this paper we assume that p is a fixed prime and x, y and z are integers for which

$(2)_p$ $\qquad x^p + y^p + z^p = 0$ and p does not divide xyz.

By Lehmer's computations [**15**], we may assume $p > 6.10^9$.

For $t \in \mathbf{Q}$ let

$$F_t(X) = \frac{1}{1-te^X} = \sum_{n\geq 0} f_n(t)\frac{X^n}{n!}$$

and let

$$B(X) = \frac{X}{e^X - 1} = \sum_{n\geq 0} B_n \frac{X^n}{n!}.$$

Let $\xi = \xi_p = \cos 2\pi/p + i \sin 2\pi/p$. Let $A = \mathbf{Z}[\xi]$ and $K = \mathbf{Q}(\xi)$. For given integer a, not divisible by p, define the Fermat quotient, $q_p(a) = (a^{p-1} - 1)/p$.

Let H_p be the set of pairs of integers (x, y) with the following properties:

(i) $\gcd(x, y) = 1$.

(ii) p does not divide x, y or $x + y$.

(iii) $(x + y)^{p-1} \equiv 1 \pmod{p^2}$.

(iv) $(x + \xi y)$ is the pth power of an ideal of K.

It is easy to show, by use of the theorem of unique factorization of ideals in $\mathbf{Q}(\xi)$ that if $(2)_p$ has solutions x, y, z then p divides $x+y+z$ and (x,y), (y,z) and (z,x) are elements of H_p.

We conjecture the following for primes $p > 6 \times 10^9$.

CONJECTURE 1_p. *There do not exist integers x, y, z such that p divides $x+y+z$ and (x,y), (y,z) and (z,x) are elements of H_p.*

It is clear that if Conjecture 1_p holds then $(2)_p$ has no solutions.

We make a number of definitions:

Let H_p^* be the set of congruence classes $(\mathrm{mod}\, p)$ of $-y/x$ where $(x,y) \in H_p$.

Let H_p^+ be the set of pairs (t,u) of congruence classes $(\mathrm{mod}\, p)$ for which there exists (x,y), $(w,z) \in H_p$ such that $t \equiv -y/x \ (\mathrm{mod}\, p)$, $u \equiv -z/w \ (\mathrm{mod}\, p)$ and at least $p-3$ of the conjugates of $x+\xi y$ are prime to $w+\xi z$ in A.

We make a large number of simple observations.

LEMMA 7. *If $(x,y) \in H_p$ then*

(i) (y,x), $(-x,-y) \in H_p$.

(ii) *The ideals $(x+\xi^a y)$ $(1 \le a \le p-1)$ are each pth powers of ideals of K, and are pairwise coprime in A.*

(iii) $(1,1) \in H_p$ *iff* p^2 *divides* $2^{p-1}-1$.

(iv) *If p divides $q_p(2)$ then*

(a) $-1 \in H_p^*$.

(b) *If $t \in H_p^*$ then $(-1,t) \in H_p^+$.*

(v) *If $t \in H_p^*$ then $t^{-1} \in H_p^*$ and $(t,t) \in H_p^+$.*

(vi) *If $(t,u) \in H_p^+$ then $(u,t), (t^{-1},u) \in H_p^+$.*

(vii) *Suppose x, y, z is a solution of $(2)_p$. Then*

(a) (x,y), (y,z), $(z,x) \in H_p$.

(b) *For each $t \in G$, $t \in H_p^*$.*

(c) *For each u, $t \in G$, $(u,t) \in H_p^+$.*

PROOF. (i) Trivial.

(ii) There exists an ideal I of K such that $(x+\xi y) = I^p$. For $1 \le a \le p-1$, let $\sigma_a : K \to K$ be the automorphism that fixes $\mathbf{Q}$ and $\sigma_a(\xi) = \xi^a$. Then $(x+\xi^a y) = \sigma_a((x+\xi y)) = \sigma_a(I^p) = (\sigma_a I)^p$.

Now suppose L is a prime ideal of A such that L divides $(x+\xi^a y)$ and $(x+\xi^b y)$. As $\xi^b(\xi^{a-b}-1)/(\xi-1)$ is a unit of A, and

$$\xi^b \left(\frac{\xi^{a-b}-1}{\xi-1} \right) (\xi-1)y = (x+\xi^a y) - (x+\xi^b y),$$

we know that $\xi - 1 \cdot y \in L$.

If $y \in L$ then $x \in L$, as $x+\xi^a y \in L$, so that $N_{K|\mathbf{Q}}(L)$ divides $\gcd(x,y) = 1$ which gives a contradiction.

Thus $\xi - 1 \in L$. But then $L = (\xi-1)$ as $(\xi-1)$ is a prime ideal of A. As $x+\xi^a y \in (\xi-1)$ we have $x+y \in (\xi-1)$ but then $p = N_{K|\mathbf{Q}}(\xi-1)$ divides $x+y$ contrary to hypothesis.

(iii) $(1+\xi)$ is precisely the ideal of units of K so that $(1+\xi)^p = (1+\xi)$. Thus, by definition,

$$(1,1) \in H_p \quad \text{if and only if} \quad 2^{p-1} \equiv 1 \pmod{p^2}.$$

(iv) is trivial from (iii).

(v) follows immediately from (i) and (ii).

(vi) is trivial from definitions.

(vii) (a) and (b) are immediate from definitions. (t,t) and $(t,t^{-1}) \in H_p^+$ by (v) and (vi).

Suppose $u \in G$ and $u \not\equiv t$ or $t^{-1} \pmod p$; then, without loss of generality, $t \equiv -y/x \pmod p$ and $u \equiv -\alpha/\beta \pmod p$ where one of α and β is z, the other is x or y. Then $N(x+\xi y)$ divides z^p and $N(\beta+\xi\alpha)$ divides x^p or y^p. But $\gcd(z,xy)=1$ and so all the conjugates of $x+\xi y$ are prime to all of those of $\beta+\xi\alpha$. Thus $(u,t) \in H_p^+$.

A careful examination of the proofs of Lemmas 1, 2 and 3 (as given by Vandiver [**31**] and Hasse [**11**]) allows us to claim that each of these hold for any t in H_p^* and (u,t) in H_p^+.

We make a slightly weaker conjecture than Conjecture 1_p:

CONJECTURE 2_p. *There does not exist $t \in H_p^*$ such that $(t,1-t)$, $(t,1-1/t)$ and $(1-t,1-1/t)$ are all elements of H_p^+.*

From Lemma 7(vii), it is clear that if $(2)_p$ has solutions then Conjecture 2_p is false. Thus if Conjecture 2_p is true then $(\mathrm{FLTI})_p$ must also hold.

We do not know of any place in the literature where Conjectures 1_p or 2_p are explicitly stated. Most of the known algebraic theorems on the first case of Fermat's Last Theorem indeed come from supposing that Conjecture 1_p (or Conjecture 2_p) is false, and so we will make Conjecture 2_p the starting point of our investigations. (The theorems which come under the heading 'Sophie Germain's Theorem' make more use of the actual Fermat equation.)

We now restate Lemmas 1–3 in terms of our sets H_p^+ and H_p^*.

THEOREM 1. (i) *If $t \in H_p^*$ then $B_{p-1-n}f_n(t) \equiv 0 \pmod p$ for $n = 1,2,3,\ldots, p-2$.*

(ii) *If $(u,t) \in H_p^+$ then $f_n(t)f_{p-2-n}(u) \equiv 0 \pmod p$ for $n = 0,1,2,\ldots,p-2$.*

For our purposes it is preferable to restate Theorem 1 as follows:

THEOREM 1′. *Let $u,t \in H_p^*$, $(u,t) \in H_p^+$ and $q,r,s \in \mathbf{Z}$ such that p does not divide q. Then*

(i)
$$\left[\frac{d^{p-2}}{dX^{p-2}}F_u(rX)F_t(sX)\right]_{X=0} \equiv 0 \pmod p.$$

(ii)
$$\left[\frac{d^{p-2}}{dX^{p-2}}F_t(rX)\right]_{X=0} \equiv 0 \pmod p.$$

(iii)
$$\left[\frac{d^{p-1}}{dX^{p-1}}\frac{1}{q}B(qX)(F_t(rX)-F_t(sX))\right]_{X=0} \equiv 0 \pmod p.$$

PROOF.

(i)

$$\text{LHS} = \sum_{n=0}^{p-2} \binom{p-2}{n} r^n s^{p-2-n} f_n(u) f_{p-2-n}(t) \equiv 0 \pmod{p}$$

by Theorem 1(ii).

(ii) LHS $= r^{p-2} f_{p-2}(t)$. Now, consider Theorem 1(i) at $n = p-2$. We have

$$f_{p-2}(t) \equiv -2(-1/2) f_{p-2}(t) \equiv -2B_1 f_{p-2}(t) \equiv 0 \pmod{p}.$$

(iii)

$$\begin{aligned}\text{LHS} &= \sum_{n=0}^{p-1} \binom{p-1}{n} q^{n-1}(r^{p-1-n} - s^{p-1-n}) B_n f_{p-1-n}(t) \\ &\equiv \frac{1}{q}(r^{p-1} - s^{p-1}) f_{p-1}(t) \pmod{p} \quad \text{by Theorem 1(i)} \\ &\equiv 0 \pmod{p} \quad \text{by Lemma 6.}\end{aligned}$$

3. Algebraic preparation. If a, b and c are integers with $c > 0$ and $\gcd(b, c) = 1$ then define $\alpha(a, b, c)$, $\beta(a, b, c)$ to be the least positive, nonnegative residue of $a/b \pmod{c}$. In other words,

$$\alpha(a, b, c) \equiv \beta(a, b, c) \equiv a/b \pmod{c}$$

where $1 \le \alpha(a, b, c) \le c$ and $0 \le \beta(a, b, c) \le c - 1$.

If y is a real number then let $[y]$ be the largest integer less than or equal to y.

We now present a series of technical lemmas involving the properties of α and β.

LEMMA 8. *Suppose that a, b and c are integers with $c > 0$ and $\gcd(b, c) = 1$.*

(i) $a - c[a/c] = \beta(a, 1, c)$.

(ii) $\alpha(a, b, c) + \beta(-a, b, c) = c$.

(iii) $\alpha(a, b, c) = 1 + \beta(a - b, b, c)$.

(iv) $\{0, 1, 2, \ldots, c-1\} = \{\beta(a, b, c) : a = 0, 1, 2, \ldots, c-1\}$.

$$\{a : 1 \le a \le c-1, \gcd(a, c) = 1\} = \{\beta(a, b, c) : 1 \le a \le c-1, \gcd(a, c) = 1\}.$$

If c is prime and $\gcd(a, c) = 1$ then

$$\{1, 2, \ldots, c-1\} = \{\beta(a, b, c) : b = 1, 2, \ldots, c-1\}.$$

Henceforth assume $b > 0$.

(v) *If $1 - c \le a \le b - 1$ then $b\alpha(a, b, c) + c\beta(a, c, b) = a + bc$.*

(vi) *If $b > c$ and $0 < a < b$ then*

$$\alpha(a, b, c) + \beta(a, c, b) = c + \alpha(a, b, b - c)$$

and

$$\alpha(a, b, c) - \beta(a, c, b) = -b + \alpha(a, b, b + c).$$

PROOF. (i), (ii), (iii) and (iv) follow immediately from definitions. Now let $\alpha = \alpha(a, b, c)$, $\beta = \beta(a, c, b)$.

(v) $b\alpha + c\beta - bc \equiv c\beta \equiv a \pmod{b}$ and $b\alpha + c\beta - bc \equiv b\alpha \equiv a \pmod{c}$, so that $b\alpha + c\beta - bc \equiv a \pmod{bc}$. But $b - bc \le b\alpha + c\beta - bc \le bc + c(b-1) - bc = bc - c$, so that $b\alpha + c\beta - bc = a$.

(vi) As $0 < a < b$, $\beta \geq 1$ and, by (v), $a = b\alpha + c\beta - bc$. Now

$$\alpha + \beta - b = \alpha - (b - \beta) \leq \alpha - (b - \beta)c/b = (\alpha b + \beta c - bc)/b = a/b < 1$$

and $\alpha + \beta \geq (\alpha b + \beta c)/b = a/b + c > c$, so that $b - c \geq \alpha + \beta - c > 0$. But

$$\alpha(a, b, b - c) \equiv a/b \equiv \alpha + c\beta/b - c \equiv \alpha + \beta - c \pmod{b - c}$$

so that $\alpha(a, b, b - c) = \alpha + \beta - c$. Now

$$c \geq c + a/b - 1 = (a + bc)/b - 1 = \alpha - 1 + \beta c/b > \alpha - 1 \geq \alpha - \beta$$

and $\alpha - \beta > -\beta \geq -b$, so that $b + c > b + \alpha - \beta > 0$. But

$$\alpha(a, b, b + c) \equiv a/b = \alpha - c + c\beta/b \equiv b + \alpha - \beta \pmod{b + c}$$

so that $\alpha(a, b, b + c) = b + \alpha - \beta$.

THEOREM 2. *If r and s are coprime positive integers, u and t are nonzero real numbers and X an indeterminate then*

$$\frac{u^s - t^r}{(1 - uX^r)(1 - tX^s)} \equiv \sum_{i=0}^{r-1} u^{\alpha(i,r,s)} t^{\beta(i,s,r)} \frac{X^i}{1 - uX^r} - \sum_{j=0}^{s-1} t^{\alpha(j,s,r)} u^{\beta(j,r,s)} \frac{X^j}{1 - tX^s}.$$

PROOF. We let

$$V(X) = V_{r,s,t,u}(X) = (1 - tX^s) \sum_{i=0}^{r-1} u^{\alpha(i,r,s)} t^{\beta(i,s,r)} X^i - (1 - uX^r) \sum_{j=0}^{s-1} t^{\alpha(j,s,r)} u^{\beta(j,r,s)} X^j + t^r - u^s,$$

which is a polynomial in $\mathbf{R}[X]$ of degree $r + s - 1$. We will show that $V(x)$ has $r + s$ distinct zeros, so that $V(X)$ is identically zero, and the theorem follows from dividing through by $(1 - uX^r)(1 - tX^s)$. If y is a root of $X^s - t^{-1}$ then

$$\begin{aligned} V(y) + u^s - t^r &= (uy^r - 1) \sum_{j=0}^{s-1} y^{-s\alpha(j,s,r)} u^{\beta(j,r,s)} y^j \\ &= (uy^r - 1) \sum_{j=0}^{s-1} (uy^r)^{\beta(j,r,s)} y^{-rs} \quad \text{(by Lemma 8(v))} \\ &= t^r (uy^r - 1) \sum_{k=0}^{s-1} (uy^r)^k \quad \text{(by Lemma 8(iv))} \\ &= t^r (u^s y^{rs} - 1) = u^s - t^r. \end{aligned}$$

Therefore $V(y) = 0$ for each y such that $y^s = t^{-1}$ and similarly $V(z) = 0$ for each z such that $z^r = u^{-1}$. It is clear that these give sets of s and r distinct roots respectively. If $y_0 = z_0$ and $y_1 = z_1$ are distinct roots of both equations, then $(y_0/y_1)^s = 1$ and $(y_0/y_1)^r = (z_0/z_1)^r = 1$. But, as $\gcd(r, s) = 1$, this implies that $y_0/y_1 = 1$, contradicting the fact that y_0 and y_1 are distinct.

Therefore $X^s - t^{-1}$ and $X^r - u^{-1}$ have at most one root in common; and so we have now found at least $r + s - 1$ distinct roots of $V(x)$. Finally as $V(0) = (1\,u^s\,t^0) - (1\,t^r\,u^0) + t^r - u^s = 0$ we have exhibited at least $r + s$ distinct roots of $V(X)$ and the result follows.

For nonzero real numbers t and u, indeterminate X and integers i, r and s we make the following definitions:

$$F_t(X) = \frac{1}{1 - te^X} = \sum_{n\geq 0} f_n(t)\frac{X^n}{n!};$$

$$W_{t,i,r}(X) = \frac{e^{iX}}{1 - te^{rX}} = \sum_{n\geq 0} W_{i,r}^{(n)}(t)\frac{X^n}{n!},$$

$$W_{i,r}(t) = W_{i,r}^{(p-2)}(t);$$

$$B(X) = \frac{X}{e^X - 1} = \sum_{n\geq 0} B_n\frac{X^n}{n!};$$

$$C_{t,r,s}(X) = \sum_{j=0}^{r-1} X\frac{(e^{jX} - 1)}{e^{rX} - 1}t^{\beta(j,s,r)},$$

$$C_{r,s}(t) = \left[\frac{d^{p-1}}{dX^{p-1}}C_{t,r,s}(X)\right]_{X=0};$$

$$A_{t,u,r,s}(X) = \sum_{j=1}^{s-1} t^{\alpha(j,s,r)}u^{\beta(j,r,s)}W_{t,j,s}(X),$$

$$A_{r,s}(t,u) = \left[\frac{d^{p-2}}{dX^{p-2}}A_{t,u,r,s}(X)\right]_{X=0}.$$

Let $A_{t,r,s}(X) = A_{t,1,r,s}(X)$ and $A_{r,s}(t) = A_{r,s}(t,1)$. We have many observations to make about these power series!

LEMMA 9.

(i)

$$F_t(X) + F_{t^{-1}}(-X) = 1.$$

$$f_n(t) + (-1)^n f_n(t^{-1}) = \begin{cases} 1, & n = 0, \\ 0, & n > 0. \end{cases}$$

(ii)

$$tW_{t,i,r}(X) + W_{t^{-1},r-i,r}(-X) = 0,$$

$$tW_{i,r}^{(n)}(t) + (-1)^n W_{r-i,r}^{(n)}(t^{-1}) = 0.$$

(iii)

$$W_{t,0,r}(X) = 1 + tW_{t,r,r}(X),$$

(iv)

$$W_{t,id,rd}(X) = W_{t,i,r}(dX)\colon W_{id,rd}(t) = d^{p-2}W_{i,r}(t).$$

(v)

$$W_{t,0,1}(X) = F_t(X).$$

(vi)

$$B(X) - B(-X) = -X.$$

Thus if n is odd then $B_n = \begin{cases} -1/2, & n=1, \\ 0, & n>1. \end{cases}$

(vii) *If $r \neq s$,*

$$B((r-s)X)(F_t(rX) - F_t(sX)) = (r-s)XF_t(rX)(F_t(sX) - 1).$$

(viii)

$$XF_1(X) + B_1(X) = 0.$$

(ix)

$$C_{t,r,s}(X) = C_{t,r,r+s}(X): \qquad C_{r,s}(t) = C_{r,r+s}(t).$$

(x)

$$XA_{1,t,s,r}(X) + C_{t,r,s}(X) + \frac{1}{r}\frac{t^r - t}{t-1}B(rX) = 0.$$

These observations are all immediate from the definitions.

LEMMA 10.

(i)

$$C_{t,r,s}(X) - C_{t,r,r-s}(-X) = \frac{t^r - t}{t-1}X,$$
$$C_{r,s}(t) = C_{r,r-s}(t).$$

(ii) *If r is prime,*

$$\sum_{s=1}^{r-1} C_{t,r,s}(X) = \frac{t - t^r}{t-1}(B(rX) - B(X))$$

and

$$\sum_{s=1}^{(r-1)/2} C_{r,s}(t) = \frac{1}{2}\frac{t - t^r}{t-1}B_{p-1}(r^{p-1} - 1)$$
$$\equiv \frac{1}{2}\frac{t^r - t}{t-1}q_p(r) \pmod{p}.$$

PROOF.

(i)

$$C_{t,r,r-s}(-X) = -X\sum_{j=1}^{r-1}\frac{e^{-jX} - 1}{e^{-rX} - 1}t^{\beta(j,r-s,r)}$$
$$= X\sum_{j=1}^{r-1}\frac{(e^{(r-j)X} - 1 + 1 - e^{rX})}{e^{rX} - 1}t^{\beta(r-j,s,r)}$$
$$= X\sum_{j=1}^{r-1}\left(\frac{e^{jX} - 1}{e^{rX} - 1} - 1\right)t^{\beta(j,s,r)}$$
$$= C_{t,r,s}(X) - X\frac{t^r - t}{t-1} \quad \text{(by Lemma 8(iv))}.$$

(ii)

$$\sum_{s=1}^{r-1} C_{t,r,s}(X) = X \sum_{j=0}^{r-1} \frac{e^{jX}-1}{e^{rX}-1} \sum_{s=1}^{r-1} t^{\beta(j,s,r)}$$
$$= \frac{X}{e^{rX}-1} \frac{t^r - t}{t-1} \left(\frac{e^{rX}-1}{e^X - 1} - r \right)$$
$$= \frac{t-t^r}{t-1}(B(rX) - B(X)).$$

Now

$$2 \sum_{s=1}^{(r-1)/2} C_{r,s}(t) = \sum_{s=1}^{r-1} C_{r,s}(t) \quad \text{(by (i))}$$
$$= \frac{t-t^r}{t-1} B_{p-1}(r^{p-1} - 1) = \frac{t^r - t}{t-1}(-pB_{p-1})q_p(r).$$

Now the Von Staudt-Clausen Theorem states that $pB_{p-1} \equiv -1 \pmod{p}$ and so the result follows.

LEMMA 11. *If r and s are positive coprime integers, u and t are nonzero real numbers and X is an indeterminate then*

(i)

$$(u^s - t^r)F_u(rX)F_t(sX) + t^r F_t(sX) - u^s F_u(rX) = A_{u,t,s,r}(X) - A_{t,u,r,s}(X).$$

(ii)

$$XA_{t,r,s}(X) + C_{t,r,s}(X) + Xt^r F_t(sX) + \frac{t^r - 1}{r} B(rX)(F_t(sX) - F_t(0)) = 0.$$

PROOF. (i) Take $X = e^X$ in Theorem 2.

(ii) Take $u = 1$ in (i) and multiply through by X. Then the result follows immediately from Lemma 9(viii), (x).

LEMMA 12. *If d, r and s are positive coprime integers, t is a nonzero real number and X an indeterminate then*

(i) *If d divides $r - s$ then*

$$A_{t,d,r}(X) - A_{t,d,s}(X) = (F_t(sX) - F_t(rX)) \left(t^d + (t^d - 1) \frac{B(dX)}{dX} \right).$$

(ii) *If d divides $r + s$ then*

$$A_{t,d,r}(X) + A_{t,d,s}(-X) = (F_t(-sX) - F_t(rX)) \left(t^d + (t^d - 1) \frac{B(dX)}{dX} \right)$$
$$+ 1 - (1 + t^d)F_t(-sX).$$

PROOF. (i) By Lemma 9(ix), $C_{t,d,s+d}(X) = C_{t,d,s}(X)$. Therefore, by Lemma 11(ii),

$$A_{t,d,s+d}(X) + t^d F_t((s+d)X) + (t^d - 1) \frac{B(dX)}{dX} (F_t((s+d)X) - F_t(0))$$
$$= A_{t,d,s}(X) + t^d F_t(sX) + (t^d - 1) \frac{B(dX)}{dX} (F_t(sX) - F_t(0)).$$

Therefore

$$A_{t,d,s+d}(X) - A_{t,d,s}(X) = (F_t(sX) - F_t((s+d)X)) \left(t^d + (t^d - 1)\frac{B(dX)}{dX} \right).$$

Now summing for $s = s, s+d, \dots, r-d$ we get the result.

(ii) By Lemma 10(i),

$$C_{t,r+s,r}(X) - C_{t,r+s,s}(-X) = \frac{t^{r+s} - t}{t-1} X.$$

Note that by Lemma 9(vi), $B(-kX) = B(kX) + kX$ so that, by Lemma 11(ii),

$$\begin{aligned} \frac{t^{r+s} - t}{t-1} X = & \left[-XA_{t,r+s,s}(-X) - Xt^{r+s}F_t(-sX) \right. \\ & \left. + \frac{t^{r+s} - 1}{r+s}((r+s)X + B((r+s)X))(F_t(-sX) - F_t(0)) \right] \\ & - \left[XA_{t,r+s,r}(X) + Xt^{r+s}F_t(rX) \right. \\ & \left. + \frac{t^{r+s} - 1}{r+s} B((r+s)X)(F_t(rX) - F_t(0)) \right]. \end{aligned}$$

Now suppose that d divides $r+s$. Let $r_0 = \beta(r, 1, d)$ and $s_0 = \beta(s, 1, d)$. As d is coprime to r and s, $r_0 + s_0 = d$. Also note that d divides $r - r_0$ and $s - s_0$. So applying (i) we get

$$A_{t,d,r}(X) - A_{t,d,r_0}(X) = (F_t(r_0X) - F_t(rX)) \left(t^d + (t^d - 1)\frac{B(dX)}{dX} \right).$$

Applying the above for $r = r_0$, $s = s_0$, $d = r_0 + s_0$ we get

$$\begin{aligned} A_{t,d,r_0}(X) + A_{t,d,s_0}(-X) = & (t^d - 1)\frac{B(dX)}{dX}(F_t(-s_0X) - F_t(r_0X)) \\ & + 1 - F_t(-s_0X) - t^dF_t(r_0X). \end{aligned}$$

Note that

$$t^d + (t^d - 1)\frac{B(-dX)}{-dX} = 1 - (t^d - 1)\frac{B(dX)}{dX}$$

by Lemma 9(vi). Thus by (i)

$$A_{t,d,s}(-X) - A_{t,d,s_0}(-X) = (F_t(-s_0X) - F_t(-sX)) \left(1 - (t^d - 1)\frac{B(dX)}{dX} \right).$$

The result follows from adding the three equations above.

4. The order of t (mod p). Pollaczek [**24**], claimed to have proved that if $t \in G$ (as defined in Lemma 1) then t cannot have order 3 or 6 (mod p). Morishima [**22**] claimed to have proved that t cannot have order 4 (mod p). Unfortunately both of their proofs are incorrect as they rely on an invalid induction hypothesis. Gunderson [**10**, Theorem I], however, managed to repair both of these proofs, in his thesis, in a beautiful and ingenious way. Gunderson's proof is indeed valid for all elements of the set H_p^*, so we may state the following lemma.

LEMMA 13. *If* $t \in H_p^*$ *then* $t^2 + 1 \not\equiv 0 \pmod{p}$, $t^2 + t + 1 \not\equiv 0 \pmod{p}$ *and* $t^2 - t + 1 \not\equiv 0 \pmod{p}$.

In other words, t cannot have order 3, 4 or 6 $(\mathrm{mod}\, p)$. As pointed out by Gunderson, it does not seem that the method of proof can be extended to other orders of t.

A major error concerning the order of t $(\mathrm{mod}\, p)$ has occurred in all the papers up to date. In the hypotheses used it is continually necessary to show that there exists $t \in G$ such that t has 'sufficiently large' order $(\mathrm{mod}\, p)$. This is guaranteed by the following lemma of Pollaczek [**24**].

LEMMA 14. *Suppose that* t *is an integer such that* $t \not\equiv 0$ *or* $1 \pmod{p}$ *and* t *does not have order* 3 *or* 6 $(\mathrm{mod}\, p)$. *Then at least one of* t, $1 - t$ *has order* $> \sqrt{3 \log p / \log \alpha}$ *where* $\alpha = (1 + \sqrt{5})/2$.

In fact Pollaczek showed that if t has order i and $1 - t$ has order j then $ij \geq 3 \log p / \log \alpha$.

We note that when considering the set G it seems sensible to state the following.

LEMMA 15. *Suppose* $t \in G$ *and* $t_1 = t$ *has order* i, $t_2 = 1 - t$ *has order* j *and* $t_3 = t/(t-1)$ *has order* k $(\mathrm{mod}\, p)$. *Then* ij, ik, jk *are each* $\geq 3 \log p / \log \alpha$.

PROOF. Note if p does not divide u then u^{-1} has the same order as u $(\mathrm{mod}\, p)$. But $t_1 + t_2 = t_1^{-1} + t_3^{-1} = t_2^{-1} + t_3 = 1$ and so the result follows immediately from Lemma 14. (Note that $G = \{t_1, t_1^{-1}, t_2, t_2^{-1}, t_3, t_3^{-1}\}$.)

As mentioned in the introduction, all of Pollaczek's results have been proved only under the assumption that there exists $t \in G$ such that t does not have order k $(\mathrm{mod}\, p)$ for certain values of k. By Lemma 14 this is certainly true for $p > \alpha^{k^2/3}$. However all these previous authors [**10**, **22**, **24**, **28**] have stated their results unconditionally: the justification being that they show that there exists $t \in G$ that does not have order k $(\mathrm{mod}\, p)$. This is a mistake. To rephrase this more clearly: Let K be a set of integers. What needs to be shown is that:

There exists $t \in G$ such that t does not have order k $(\mathrm{mod}\, p)$ for each $k \in K$. What has been shown is that:

For each $k \in K$, there exists $t \in G$ such that t does not have order k $(\mathrm{mod}\, p)$. (Note, in the first it is the *same* t in each case, in the second it can be a *different* t in different cases.)

It is not hard to see that either the six elements of the set G are distinct $(\mathrm{mod}\, p)$ or

(i) There exists $t \in G$ such that $t^2 - t + 1 \equiv 0 \pmod{p}$ or

(ii) $G = \{-1, 2, 1/2\}$.

By Lemma 13, we know that (i) cannot hold and so we have two cases:

(A) G has six distinct elements $(\mathrm{mod}\, p)$.

(B) The elements of G are -1, 2 and $1/2$ $(\mathrm{mod}\, p)$.

5. Algebra for the first case.

LEMMA 16. *Suppose* $(u,t) \in H_p^+$, r,s *are coprime positive integers. Then*
(i) $A_{r,s}(t,u) \equiv A_{s,r}(u,t) \pmod p$.
(ii) $C_{r,s}(t) \equiv A_{r,s}(t) \pmod p$.
(iii) *If* d *divides* $r-s$ *or* $r+s$ *then* $A_{d,r}(t) \equiv A_{d,s}(t) \pmod p$.

PROOF. We apply Theorem 1′ directly to Lemmas 11 and 12, taking the $(p-2)$nd differential with respect to X (for (i) and (ii)), and multiplying by X and taking the $(p-1)$st differential with respect to X (for (iii)) of both sides, and evaluating at $X=0$.

We now introduce the induction hypothesis that was first used by Frobenius, and then by Pollaczek, Morishima and Gunderson.

We say that $(W_{n,t})$ is true if for all integers m, $1 \le m \le n-1$, and i, $0 \le i \le m-1$, we have $W_{i,m}(t) \equiv 0 \pmod p$.

LEMMA 17. *If* $t \in H_p^*$, $(W_{n,t})$ *is true, and* r *and* s *are integers such that* $0 \le s < n$ *and* $r > 0$ *then* $A_{r,s}(t) \equiv 0 \pmod p$ *and* $C_{r,s}(t) \equiv 0 \pmod p$. *If* $(u,t) \in H_p^*$ *then* $A_{r,s}(t,u) = 0 \pmod p$.

PROOF. Immediate from definitions of $A_{r,s}(t,u)$ and by Lemma 16.

LEMMA 18. *Suppose that* n *is a positive integer,* $t \in H_p^*$ *and* $(W_{n,t})$ *is true. If* $1 \le m < n$, $r = 2m+1$ *is prime and* $t^{2m} \not\equiv 1 \pmod p$ *then* $q_p(r) \equiv 0$ (*i.e.* p^2 *divides* $r^p - r$).

PROOF. Immediate from Lemma 17 and Lemma 10(ii).

THEOREM 3. *If* $t \in H_p^*$ *then* $(W_{4,t})$ *is true and if* $t \not\equiv -1 \pmod p$, p^2 *divides* $r^p - r$ *for* $r = 2, 3, 5$ *and* 7.

PROOF. By Lemma 9(iv) and (v), $(W_{4,t})$ is true if and only if $f_{p-2}(t) \equiv W_{r,s}(t) \equiv 0 \pmod p$ for $(r,s) = (1,2), (1,3)\&(2,3)$. By Theorem 1′, we know that $f_{p-2}(t) \equiv 0 \pmod p$. Now

$$\begin{aligned} W_{1,2}(t) &= t^{-1}A_{1,2}(t) \quad \text{(by definition)} \\ &\equiv t^{-1}A_{1,1}(t) \equiv 0 \pmod p \quad \text{(by Lemma 16(iii))}. \end{aligned}$$

Now

$$tW_{1,3}(t) + tW_{2,3}(t) = A_{1,3}(t) \equiv A_{1,2}(t) \equiv 0 \pmod p$$

and

$$tW_{1,3}(t) + t^2W_{2,3}(t) = A_{2,3}(t) \equiv A_{2,1}(t) \equiv 0 \pmod p.$$

But as $t \not\equiv 0$ or $1 \pmod p$, $W_{1,3}(t) \equiv W_{2,3}(t) \equiv 0 \pmod p$. Thus $(W_{4,t})$ is true.

Now, by Lemma 13, we see that t does not have order $3, 4$ or $6 \pmod p$. Thus, as $t \not\equiv -1$ or $1 \pmod p$, we know that

$$t^2 \not\equiv 1 \pmod p,\ t^4 \not\equiv 1 \pmod p \text{ and } t^6 \not\equiv 1 \pmod p.$$

So, by Lemma 18, p^2 divides $r^p - r$ for $r = 3, 5$ and 7. Finally, note that, by Lemmas 10(ii) and 16,

$$t(-pB_{p-1})\frac{2^{p-1}-1}{p} = C_{2,1}(t) \equiv 0 \pmod p$$

and as $-pB_{p-1} \equiv 1 \pmod p$, we see that p^2 divides $2^p - 2$.

LEMMA 19. *If $u \in H_p^*$ and $(W_{n,u})$ is true then $u^{-1} \in H_p^*$ and $(W_{n,u^{-1}})$ is also true.*

PROOF. $u^{-1} \in H_p^*$ by Lemma 7(v) and $(W_{n,u^{-1}})$ is true follows immediately from Lemma 9(i) and (ii).

THEOREM 4. (a) *Suppose $t \in H_p^*$ and that $(W_{n,t})$ is true for some positive integer n. Then, for $1 \le m \le 2n-1$, $\gcd(m,n) = 1$,*

$$\sum_{\substack{j=1 \\ \gcd(j,n)=1}}^{n-1} t^{\alpha(j,n,m)} W_{j,n}(t) \equiv 0 \pmod{p}.$$

(b) *If $u \in H_p^*$, $(u,t) \in H_p^+$ and $(W_{n,u})$ is also true then, for $1 \le m \le n-1$, $\gcd(m,n) = 1$, $\delta = -1$ or 1*

$$\sum_{\substack{j=1 \\ \gcd(j,n)=1}}^{n-1} t^{\alpha(j,n,m)} u^{\delta\beta(j,m,n)} W_{j,n}(t) \equiv 0 \pmod{p}.$$

PROOF. Note that if $\gcd(k,n) \ne 1$, then $W_{k,n}(t) \equiv 0 \pmod{p}$ by Lemma 9(iv).

(a) If $m < n$, let $r = n - m$ and so m divides $n - r$.

If $m > n$, let $r = m - n$ and so m divides $n + r$. In both cases $r < n$, $\gcd(r,n) = 1$ and so by Lemma 16(iii)

$$A_{m,n}(t) \equiv A_{m,r}(t) \equiv 0 \pmod{p}.$$

(b) By Lemma 19, $(W_{n,u^{-1}})$ is true. So, by Lemma 16(i),

$$A_{m,n}(t, u^{\delta}) \equiv A_{n,m}(u^{\delta}, t) \equiv 0 \pmod{p}.$$

REMARK. Taking $u = t$ or t^{-1} in Theorem 4(b), gives the equations of Theorem 4(a) by application of Lemma 8(vi).

6. The theory of the computations. Our objective is to establish that p^2 divides $r^p - r$ for primes $r = 2, 3, 5, 7, 11, 13, \ldots$. We do this by successively establishing that $(W_{1,t})$, $(W_{2,t}), \ldots, (W_{k,t}), \ldots$ are true for all t in some subset S of H_p^*: and then by using Lemma 18 with some $t \in S$ for which $t^{r-1} \not\equiv 1 \pmod{p}$.

Previous authors have simply chosen $t \in G$ with highest order $\pmod{p}$ and let $S = \{t, t^{-1}\}$ (see Lemma 19).

If $(W_{n,t})$ is true then, in order to establish $(W_{n+1,t})$, we have by Theorem 4(a) $2\phi(n)$ equations to solve $\pmod{p}$, in the $\phi(n)$ unknowns $W_{1,n}(t), \ldots, W_{n-1,n}(t)$.

Let $1 = k_1 < k_2 < \cdots < k_{\phi(n)} = n - 1 < \cdots < k_{2\phi(n)} = 2n - 1$ be the sequence of integers between 1 and $2n$ that are prime to n. Let $\mathbf{A}_n$ be the $2\phi(n) \times \phi(n)$ matrix with (i,j)th entry $X^{\alpha(k_j,n,k_i)}$. Let $\mathbf{W}_n$ be the $\phi(n) \times 1$ column vector

$$(W_{k_1,n}(X), W_{k_2,n}(X), \ldots, W_{k_{\phi(n)},n}(X))^{\mathrm{T}}$$

and $\mathbf{0}$ be the $2\phi(n) \times 1$ zero column vector. We may re-express Theorem 4(a) as

$$\mathbf{A}_n \mathbf{W}_n(t) \equiv \mathbf{0} \pmod{p}.$$

It is clear that the statement $(W_{n,t})$ is true is precisely the statement that $\mathbf{W}_m(t) \equiv \mathbf{0} \pmod{p}$ for each m, $1 \le m < n$.

The best way to establish $(W_{n+1,t})$ would be to solve the system of equations above and show that it only can hold if $\mathbf{W}_n(t) \equiv \mathbf{0} \pmod p$. Unfortunately this is very far from being practical for computational purposes.

The method established by Pollaczek was as follows: Suppose that $(W_{n+1,t})$ is false so that $\mathbf{W}_n(t) \not\equiv \mathbf{0} \pmod p$. Let $\mathbf{B}$ be any $\phi(n) \times \phi(n)$ submatrix of $\mathbf{A}_n$. Then $\mathbf{B}\mathbf{W}_n(t) \equiv \mathbf{0} \pmod p$, and so $D(t) = \det \mathbf{B} \equiv 0 \pmod p$. If we find a number of such determinants $D_1, D_2, \dots, D_k$ from distinct submatrices $\mathbf{B}_1, \dots, \mathbf{B}_k$ then we know that

$$D_1(t) \equiv D_2(t) \equiv \cdots \equiv D_k(t) \equiv 0 \pmod p.$$

Before proceeding we remind the reader of the connection between the Euclidean algorithm over $\mathbf{Z}[X]$ and the resultant.

LEMMA 20. *Suppose $f, g \in \mathbf{Z}[X]$ have no common root in $\mathbf{C}$.*

(i) *There exists $a, b \in \mathbf{Z}[X]$ and a positive integer m such that $m = af + bg$.*

We define $\hat{R}(f,g)$ to be the minimum such m.

(ii) *If p is a prime then there exists $h \in \mathbf{Z}[X]$ such that h divides both f and g in $(\mathbf{Z}/p\mathbf{Z})[X]$ if and only if p divides $\hat{R}(f,g)$.*

The resultant $R(f,g)$ is defined as follows: If $f = a\prod_{i=1}^{r}(X-\alpha_i)$ and $g = b\prod_{j=1}^{s}(X-\beta_j)$ then

$$R(f,g) = \left| a^s b^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\alpha_i - \beta_j) \right| \qquad \left(= \left| b^r \prod_{j=1}^{s} f(\beta_j) \right| \right).$$

(iii) $R(f,g) \le \|f\|_2^s \|g\|_2^r$ *($\|f\|_2^2$ is defined to be the sum of the squares of the coefficients of f).*

(iv) *$\hat{R}(f,g)$ divides $R(f,g)$.*

For more details of Lemma 20, see [**29**].

Now, returning to our problem, let $g_{ij}(X) = \gcd_{\mathbf{Q}[X]}(D_i, D_j)$. Then either $g_{ij}(t) \equiv 0 \pmod p$ or, by Lemma 20(ii), p divides $\hat{R}(D_i/g_{ij}, D_j/g_{ij})$. It turns out that, in practice, the polynomials g_{ij} are simply products of cyclotomic polynomials of low order; therefore if $t^m \not\equiv 1 \pmod p$ for all 'small' values of m, then p divides $\gcd_{i,j} \hat{R}(D_i/g_{ij}, D_j/g_{ij})$ which we can directly factor. This method works very well for $n \le 16$.

In our hypothesis by taking a larger set S (for instance $S = G$) we get many more equations ($|S|\phi(n)$) by applying Theorem 4(b), which makes the computations easier. Furthermore it turns out that, by using our technique, it is easy to show that $(W_{n,t})$ holds for t of any order $\pmod p$ (but not $1, 3, 4$ or 6), which is not the case with Pollaczek's method. For instance, if $n = 14$, $\phi(n) = 6$ and t has order $8 \pmod p$ then the matrix $\mathbf{A}_n$ has rank $5 \pmod p$, and so by Pollaczek's method one has to assume that $p > \alpha^{64/3}$ (see Lemma 14).

Suppose that we have shown that $(W_{n,t})$ is true for each $t \in G$ $(= S)$; and $r = 2m+1$ is prime where $1 \le m < n$. In order to use Lemma 18 we need to show that there exists $t \in G$ such that $t^{2m} \not\equiv 1 \pmod p$.

LEMMA 21. *Let m be a positive integer. If 3 divides m let*

$$R_m = \hat{R}\left(\frac{X^{2m}-1}{X^6-1}, \frac{(X-1)^{2m}-1}{(X-1)^6-1} \right);$$

otherwise let

$$R_m = \hat{R}(X^{2m} - 1, (X-1)^{2m} - 1).$$

If p is a prime such that $t^{2m} \equiv 1 \pmod{p}$ for each $t \in G$, then p divides R_m.

The proof of this is immediate from the definition of G and Lemma 13.

We computed R_m for each $m \leq 54$ such that $2m+1$ is prime. In Table III we list the prime factors of R_m that are greater than 10^6. The factorizations of the R_m were done by using Pollard's rho algorithm [**25**]. We then used Wieferich's test on each of these primes and showed, in each case, that p^2 does not divide $2^p - 2$ (see Lemma 4).

7. Problems with the theory of the computations in practice. A straightforward approach to the computations leads to the manipulation of polynomials of very high degree, which becomes prohibitively expensive. We have found a number of techniques to reduce the degrees of the polynomials involved. For instance, the computation of the resultant of polynomials f and g of degree d, involves an algorithm of order d^4. If $f = f_1 f_2$ and $g = g_1 g_2$ where each f_i and g_i has degree $d/2$ then by taking

$$R(f,g) = R(f_1,g_1)R(f_1,g_2)R(f_2,g_1)R(f_2,g_2)$$

we reduce the cost by a factor of 4.

In Lemma 22 we make a general observation about $\hat{R}(f,g)$ and, in Lemma 23, we apply this to two specific cases. Each case allowed us, in our computations, to reduce costs by a factor of 16.

LEMMA 22. *Suppose f, g and $h \in \mathbf{Z}[X]$ and k is an integer. Let $F(X) = X^{k\cdot df} f(h(X)X^{-k})$ and $G(X) = X^{k\cdot dg} g(h(X)X^{-k})$ where df, dg are the degrees of f and g respectively. If p is a prime and t is an integer, not divisible by p, such that $F(t) \equiv G(t) \equiv 0 \pmod{p}$, then p divides $\hat{R}(f,g)$.*

PROOF. Let $u = h(t)/t^k$. Then $f(u) \equiv t^{-k\cdot df} F(t) \equiv 0 \pmod{p}$, and similarly $g(u) \equiv 0 \pmod{p}$. But then, by Lemma 20(ii), p divides $\hat{R}(f,g)$.

As an immediate corollary we may state

LEMMA 23. *Suppose F and $G \in \mathbf{Z}[X]$, p is a prime and t is an integer not divisible by p such that $F(t) \equiv G(t) \equiv 0 \pmod{p}$.*

(i) *If F and G are both even (i.e. $F(X) = f(X^2)$ and $G(X) = g(X^2)$) then p divides $\hat{R}(f,g)$.*

(ii) *If F and G are both symmetric (i.e. $F(X) = X^{df} f(X + 1/X)$ and $G(X) = X^{dg} g(X + 1/X)$) then p divides $\hat{R}(f,g)$.*

In computations of determinants of large matrices with polynomial entries, it helps to reduce the degrees of the entries; if we can reduce these degrees by, say, a factor of 2 then, by any standard algorithm, we will make significant savings. For instance, in the first $2\phi(n)$ rows of the matrix used by Pollaczek (derived from Theorem 4(a)) there are many entries of degree greater than n. As an example take $n = 19$. If we take the determinants of four submatrices of the first 21 rows, then each such determinant will have degree approximately 200. For $n = 43$, the degrees will be approximately 850!

The matrix formed by Pollaczek is very beautiful in the sense that each entry is a power of X. However to compute subdeterminants for large values of n has been seen to be difficult. In the next section we will present a number of highly technical lemmas, which will allow us to significantly reduce the degree of Pollaczek's matrix, by removing a large number of cyclotomic factors before the computations. As an example suppose n is odd and take the rows with $m = 1$ and 2 in Theorem 4(a). We have

$$R_1 = X \sum_{\substack{j=1 \\ \gcd(j,n)=1}}^{n-1} W_{j,n}(X) \equiv 0 \pmod{p}$$

and

$$R_2 = X \sum_{\substack{j=1 \\ \gcd(j,n)=1 \\ j \text{ odd}}}^{n-1} W_{j,n}(X) + X^2 \sum_{\substack{j=1 \\ \gcd(j,n)=1 \\ j \text{ even}}}^{n-1} W_{j,n}(X) \equiv 0 \pmod{p}.$$

Now, we replace the row R_2 by the rows R_2', where

$$R_2' = (R_2 - R_1)/(X^2 - X) = \sum_{\substack{j=1 \\ \gcd(j,n)=1 \\ j \text{ even}}}^{n-1} W_{j,n}(X) \equiv 0 \pmod{p}.$$

It is apparent here that we cut the degree of the row by 2; and indeed many such savings may be made. For instance, in the $n = 43$ case, the determinants will have degree less than 425.

Typically, by the results in §8, we are able to reduce degrees by a factor of 2. Not only does this mean that the determinants are easier to compute, but also the resultants of these determinants are also easier to compute; and, ultimately, the factorization of those resultants becomes possible.

8. More algebra to reduce costs.

LEMMA 24. *Let d, r and s be coprime positive integers, t be a nonnegative real number and X be an indeterminate.*

(i) *If d divides $r - s$ and g divides d then*

$$\frac{A_{t,d,r}(X) - A_{t,g,r}(X)}{t^g - 1} - \frac{A_{t,d,s}(X) - A_{t,g,s}(X)}{t^g - 1}$$
$$= (F_t(sX) - F_t(rX)) \left(\frac{t^d - t^g}{t^g - 1} + \frac{t^d - 1}{t^g - 1} \frac{B(dX)}{dX} - \frac{B(gX)}{gX} \right).$$

(ii) *If d divides $r + s$ and g divides d then*

$$\frac{A_{t,d,r}(X) - A_{t,g,r}(X)}{t^g - 1} + \frac{A_{t,d,s}(-X) - A_{t,g,s}(-X)}{t^g - 1}$$
$$= (F_t(-sX) - F_t(rX)) \left(\frac{t^d - t^g}{t^g - 1} + \frac{t^d - 1}{t^g - 1} \frac{B(dX)}{dX} - \frac{B(gX)}{gX} \right)$$
$$- \frac{t^d - t^g}{t^g - 1} F_t(-sX).$$

PROOF. These follow immediately from Lemma 12.

We introduce, only for convenience, the following notation in Lemma 25, where d, r, s, t and X are as above.

$$V_{d,\delta}(X) = A_{t,d,r}(X) - \delta A_{t,d,s}(\delta X) \quad \text{with } \delta = -1 \text{ or } 1.$$

Note that, by Lemma 12, if d divides $r - \delta s$,

$$V_{d,\delta}(X) = (F_t(\delta sX) - F_t(rX))\left(t^d + (t^d - 1)\frac{B(dX)}{dX}\right) + \left(\frac{1-\delta}{2}\right)(1 - (1 + t^d)F_t(-sX)).$$

LEMMA 25. *Let r, s, t, X and $V_{d,\delta}(X)$ be defined as above. Suppose that d divides $r - \delta s$ and g and h are positive integers such that g and h divide d, $g > h$ and h does not divide g. Let $k = \beta(g, 1, h)$ and $l = \gcd(g, h)$. Note that l divides k and $h - k$, and h divides $g - k$. Then*

(i)

$$\frac{t^k - 1}{t^g - 1 \cdot t^h - 1}V_{d,\delta(X)} - \frac{V_{h,\delta}(X)}{t^h - 1} + \frac{t^g - t^k}{t^g - 1 \cdot t^h - 1}V_{g,\delta}(X)$$
$$= (F_t(\delta sX) - F_t(rX))\left(N\frac{B(dX)}{dX} - \frac{B(hX)}{hX} + \frac{t^g - t^k}{t^h - 1}\frac{B(gX)}{gX} + M\right) + \left(\frac{\delta - 1}{2}\right)MF_t(-sX)$$

where

$$N = \frac{t^d - 1 \cdot t^l - 1 \cdot t^k - 1}{t^g - 1 \cdot t^h - 1 \cdot t^l - 1} \quad \text{and} \quad M = N - 1 + \frac{t^g - t^k}{t^h - 1}.$$

(ii)

$$\frac{1 - t^{h-k}}{t^g - 1 \cdot t^h - 1}V_{d,\delta}(X) - \frac{t^{h-k}}{t^h - 1}V_{h,\delta}(X) + \frac{t^{g+h-k} - 1}{t^g - 1 \cdot t^h - 1}V_{g,\delta}(X)$$
$$= (F_t(\delta sX) - F_t(rX))\left(N\frac{B(dX)}{dX} - t^{h-k}\frac{B(hX)}{hX} + \frac{t^{g+h-k} - 1}{t^h - 1}\frac{B(gX)}{gX} + M\right) + \left(\frac{\delta - 1}{2}\right)MF_t(-sX)$$

where

$$N = \frac{t^d - 1 \cdot t^l - 1 \cdot 1 - t^{h-k}}{t^g - 1 \cdot t^h - 1 \cdot t^l - 1} \quad \text{and} \quad M = N + t^{g-k} - t^{h-k} + \frac{t^{g-k} - 1}{t^h - 1}.$$

This lemma follows immediately from Lemma 12.

Henceforth in this section we will let $r, s, t, d, \delta, g, h, k$ and l be defined as in Lemma 25. Let

$$U^r_{d,g}(t) = (A_{d,r}(t) - A_{g,r}(t))/(t^g - 1),$$

$$U^{r,1}_{d,g,h}(t) = \frac{(t^k - 1)A_{d,r}(t) - (t^g - 1)A_{h,r}(t) + (t^g - t^k)A_{g,r}(t)}{(t^g - 1)(t^h - 1)}$$

and

$$U^{r,2}_{d,g,h}(t) = \frac{(1 - t^{h-k})A_{d,r}(t) - (t^{g+h-k} - t^{h-k})A_{h,r}(t) + (t^{g+h-k} - 1)A_{g,r}(t)}{(t^g - 1)(t^h - 1)}.$$

LEMMA 26. *Each of* $U^r_{d,g}(t), U^{r,1}_{d,g,h}(t)$ *and* $U^{r,2}_{d,g,h}(t)$ *are polynomials in* t *with integer coefficients.*

PROOF. $\alpha(j,r,d) \equiv j/r \equiv \alpha(j,r,g) \pmod g$ as g divides d, and so

$$(*) \qquad t^g - 1 \text{ divides } t^{\alpha(j,r,d)} - t^{\alpha(j,r,g)}.$$

Thus

$$U^r_{d,g}(t) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r-1} W_{j,r}(t) \frac{t^{\alpha(j,r,d)} - t^{\alpha(j,r,g)}}{t^g - 1} \in \mathbf{Z}[t].$$

Let

$$M_j(t) = t^{\alpha(j,r,d)}(t^k - 1) - t^{\alpha(j,r,h)}(t^g - 1) - t^{\alpha(j,r,g)}(t^g - t^k)$$

so that

$$U^{r,1}_{d,g,h}(t) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r-1} W_{j,r}(t) \frac{M_j(t)}{t^g - 1 \cdot t^h - 1}.$$

Now

$$M_j(t) \equiv (t^k - 1)(t^{\alpha(j,r,d)} - t^{\alpha(j,r,g)}) \equiv 0 \bmod (t^g - 1)$$

and

$$M_j(t) \equiv (t^k - 1)(t^{\alpha(j,r,d)} - t^{\alpha(j,r,h)}) \equiv 0 \bmod (t^h - 1) \text{ by } (*).$$

Now $\gcd_{\mathbf{Z}[t]}(t^g - 1, t^h - 1) = t^l - 1$ and

$$M_j(t) = (t^k - 1)(t^{\alpha(j,r,d)} - t^{\alpha(j,r,g)}) + (t^g - 1)(t^{\alpha(j,r,g)} - t^{\alpha(j,r,h)}).$$

But $\alpha(j,r,d) \equiv \alpha(j,r,g) \equiv \alpha(j,r,h) \pmod l$ so that $(t^l - 1)^2$ divides $M_j(t)$. Thus $(t^g - 1)(t^h - 1)$ divides $M_j(t)$ for each j and so $U^{r,1}_{d,g,h}(t) \in \mathbf{Z}[t]$.

It is easy to show that $U^{r,2}_{d,g,h}(t) \in \mathbf{Z}[t]$ by exactly the same method.

LEMMA 27. *Suppose* $t \in H^*_p$, r *and* s *are coprime positive integers* $(r > s)$, $\delta = 1$ *or* -1 *and* d *divides* $r - \delta s$.

(i) *If* g *divides* d *then* $U^r_{d,g}(t) \equiv U^s_{d,g}(t) \pmod p$. *Now suppose* h *divides* d, $g > h$, h *does not divide* g *and let* $k = \beta(g,1,h)$. *Then*

(ii)

$$U^{r,j}_{d,g,h}(t) \equiv U^{s,j}_{d,g,h}(t) \pmod p \quad \textit{for } j = 1 \textit{ and } 2.$$

PROOF. Immediate from Theorem 1′ and Lemmas 25 and 26.

THEOREM 5. *With the definitions of Lemma* 27 *suppose that* $(W_{r,t})$ *is true. Then*

$$U^r_{d,g}(t) \equiv U^{r,1}_{d,g,h}(t) \equiv U^{r,2}_{d,g,h}(t) \equiv 0 \pmod p.$$

The proof of Theorem 5 is immediate from Lemma 27. Note that the definition of each such $U(t)$ is independent of s. It only really depends on the fact $0 < d < 2r$ and $\gcd(d,r) = 1$.

Now for given integers m and n, $1 \le m \le 2n-1$, with $\gcd(m,n)=1$ let

$$\begin{aligned} A^*_{m,n}(X) &= A_{m,n}(X) && \text{if } m = 1 \\ &= U^n_{m,m/p}(X) && \text{if } m \text{ is a prime power of } p \\ &= U^{n,j}_{m,m/p,m/q}(X) && \text{if } m \text{ has } \ge 2 \text{ prime factors, the} \\ & && \text{smallest two being } p < q, \text{ and with } j = 1 \\ & && \text{if } \beta(m/p, 1, m/q) \le m/2q, j = 2 \text{ otherwise.} \end{aligned}$$

In our computations we will replace $A_{m,n}(X)$ by $A^*_{m,n}(X)$ which leads to a significant reduction in the degrees of the entries of the matrix.

We note that Morishima's Satz 2 [**22**], is equivalent to showing $U^r_{d,g}(t) \equiv 0 \pmod p$ in Theorem 5 for $d = r-1$ and $r+1$.

9. The algorithms. We construct the $2\phi(n)$ by $\phi(n)$ matrix $\mathbf{A}^*_n$ as follows: For $1 \le m \le 2n-1$ with $\gcd(m,n)=1$ we have

$$A^*_{m,n}(X) = \sum_{\substack{j=1 \\ \gcd(j,n)=1}}^{n-1} f_{m,j} W_{j,n}(X)$$

for certain polynomials $f_{m,j} \in \mathbf{Z}[X]$ (by Lemma 26). Let

$$d_{m,n} = \max_j \text{ degree } f_{m,j}.$$

We reorder the set $\{k_1, \dots, k_{2\phi(n)}\}$ (as defined in §6) to $\{r_1, r_2, \dots, r_{2\phi(n)}\}$ so that $d_{r_1,n} \le d_{r_2,n} \le \cdots \le d_{r_{2\phi(n)},n}$. Let the (i,j)th entry of $\mathbf{A}^*_n$ be $f_{r_i,j}$. Then, by Theorems 4 and 5, if $(W_{n,t})$ is true, we have $\mathbf{A}^*_n(t)\mathbf{W}_n(t) \equiv \mathbf{0} \pmod p$. Let M_n be the submatrix formed by the first $\phi(n)+3$ rows of $\mathbf{A}^*_n$. We will find four subdeterminants of M_n simultaneously using the following method.

LEMMA 28. *Let L be a given positive integer and let $\mathcal{F}_L$ be the set of polynomials $f = \sum_{i=0}^d a_i X^i$ in $\mathbf{Z}[X]$ such that $L \ge 2|a_i| + 1$ for each i. Then the mapping $\varphi_L : \mathcal{F}_L \to \mathbf{Z}$, defined by $\varphi_L(f) = f(L)$, is injective.*

PROOF (SEE [**4**]). Suppose $\varphi_L(f) = \varphi_L(g)$. Then $\varphi_L(f-g) = f(L) - g(L) = 0$. Now if $f - g \ne 0$ then we may write $h = f - g = \sum_{i=0}^d a_i X^i$ where each $|a_i| \le L-1$ by definition and $a_d \ne 0$. Now $\sum_{i=0}^d a_i L^i = h(L) = 0$, so that

$$\begin{aligned} L^d \le |a_d| L^d = \left| \sum_{i=0}^{d-1} a_i L^i \right| &\le \sum_{i=0}^{d-1} |a_i| L^i \\ &\le \sum_{i=0}^{d-1} (L-1) L^i = L^d - 1 \end{aligned}$$

giving a contradiction. Thus $h = 0$ so that $f = g$.

So suppose we have an $m \times m$ matrix M, whose entries are polynomials in X. In order to compute the determinant D_M we try to find an integer L such that $D_M \in \mathcal{F}_L$. Then we compute the determinant of $M(L)$, namely $D_M(L)$. This uniquely defines $D_M(X)$ (by Lemma 27), which we can then reconstruct by a simple algorithm that inverts φ_L (similar to that used to create a p-adic expansion). The

key, then, is to find a value of L for which $D_M \in \mathcal{F}_L$; in other words, we need an easy way to find a bound on the coefficients of the determinant of a given matrix with polynomial entries. This we do by using the following theorem of Goldstein and Graham [**8**].

LEMMA 29. *Suppose A is a given $n \times n$ matrix with (i,j)th entry $\sum_{k=0}^{d} a_{i,j,k} X^k \in \mathbf{Z}[X]$. Let $w_{i,j} = \sum_{k=0}^{d} |a_{i,j,k}|$. Then*

$$\|\det A\|_2 \le \left(\prod_{i=1}^{n} \sum_{j=1}^{n} w_{i,j}^2 \right)^{1/2}.$$

We have now reduced the problem to that of finding four subdeterminants of the integer matrix $M_n(L)$, simultaneously, at a suitable integer L (this process is called 'single point evaluation'—see [**4**]). In Maple, with a matrix containing integers of arbitrary precision, it costs least to use the standard method of fraction-free Gaussian elimination outlined by Bareiss [**2**]. The algorithm avoids using gcds and selects its own pivotal elements. In this way we eliminate $\phi(n) - 1$ rows (which are not predetermined, but selected by the algorithm) and are left with 4 rows which contain $\phi(n) - 1$ zeros and an integer in the last column. Thus our four subdeterminants of M_n will contain the same first $\phi(n) - 1$ rows and four distinct last rows.

Alternatively we could compute the determinant of the matrix B by making use of modular homomorphisms, evaluation homomorphisms, Newton interpolation and the Chinese Remainder Theorem, as outlined by McClellan [**18**]. However, in the context of the Maple environment, it proves more efficient to compute in the way outlined previously.

We now have four subdeterminants of M_n, namely D_1, D_2, D_3 and D_4. Before computing $\hat{R}(D_i, D_j)$ we first divided all small cyclotomic factors out of each D_i and then tested to see whether any two had a common polynomial factor (which they never did). The cyclotomic factors (except 1, 3, 4 or 6—see Lemma 13) we stored in a set S_n (which we will deal with later). The new polynomials (that is, less the cyclotomic factors) were stored in $E_1, \ldots, E_4$.

The next stage was to choose i and j and to compute $\hat{R}(E_i, E_j)$ (which is divisible by p, by Lemma 20(ii)). We usually found that some pair of our polynomials were both even, or both symmetric or were both even and symmetric, in which case we used Lemma 23, to reduce the degree.

As an example consider the case $n = 13$. Two of our polynomials are

$$E_1 = 3x^8 - x^6 - 2x^4 - x^2 + 3$$

and

$$E_2 = x^{20} + 2x^{18} + 10x^{16} + 26x^{14} + 55x^{12} + 40x^{10} + 55x^8 + 26x^6 + 10x^4 + 2x^2 + 1.$$

Now let $F_1 = 3x^2 - x - 8$ and $F_2 = x^5 + 2x^4 + 5x^3 + 18x^2 + 30x - 8$ so that

$$E_1(x) = x^4 F_1(x^2 + 1/x^2) \quad \text{and} \quad E_2(x) = x^{10} F_2(x^2 + 1/x^2).$$

So if there exists $t \in \mathbf{Z}$ such that p divides $E_1(t)$ and $E_2(t)$ then there exists $u \in \mathbf{Z}$ such that p divides $F_1(u)$ and $F_2(u)$, and so p divides $\hat{R}(F_1, F_2) = 2^4 \cdot 3 \cdot 2957$.

An advantage of using the 'Euclidean algorithm' in $\mathbf{Z}[X]$ (in fact, the subresultant algorithm—see [**3**]) is that we may store a polynomial $h(X)$ of low degree (in each case ≤ 4) such that $h(t) \equiv 0 \pmod{p}$.

Suppose we have used the algorithm on E_1 and E_2, then we get an integer R $(= \hat{R}(E_1, E_2))$ and a polynomial $h \in \mathbf{Z}[X]$ of degree ≤ 4, such that p divides R and $h(t) \equiv 0 \pmod{R}$.

We now use a 'modular Euclidean algorithm' to compute $\hat{R}(E_i, h)$ (for $i = 3, 4$) modulo R. In other words we find $\gcd(E_i, h)$ in $\mathbf{Z}/R\mathbf{Z}[X]$. Clearly this greatly reduces the cost of these other resultant computations. But now we have p divides $R = \gcd(\hat{R}(E_1, E_2), \hat{R}(h, E_3), \hat{R}(h, E_4))$ and we may also find another polynomial $h \in \mathbf{Z}[X]$ of even lower degree, such that $h(t) \equiv 0 \pmod{p}$.

We now try to factor R. First we remove all factors less than 10^5 and then use the Pollard 'p minus 1' [**25**] and Morrison-Brillhart algorithms [**23**] to try to factor R. If we succeed then we use Wieferich's test to eliminate all the prime factors (that is, we check that p^2 does not divide $2^p - 2$—see Theorem 3).

Otherwise, if R was too large to factor (as was often the case), we simply chose another $\phi(n) + 3$ rows of $\mathbf{A}_n^*$ and computed a different set of four determinants D_1', D_2', D_3', D_4'. We then used the modular Euclidean algorithm taking each D_i' with $h \pmod{R}$.

Let $g = \gcd_{1 \leq i \leq 4}(R, \hat{R}(h, D_i'))$ so that p divides g. In each case considered, we found that g was easily factored, and for each prime factor q of g, q^2 does not divide $2^q - 2$.

So we have now shown that if t does not satisfy one of the cyclotomic polynomials in $S_n \pmod{p}$, and t is an element of H_p^* then $(W_{n,t})$ true implies that $(W_{n+1,t})$ is true.

We now must consider the cyclotomic polynomials in S_n. So suppose $\phi_m(t) \equiv 0 \pmod{p}$, and for any $\phi(n) \times \phi(n)$ submatrix B of $\mathbf{A}_n^*$, we have determinant $D_B(t) \equiv 0 \pmod{p}$.

We again use the ideas of Lemmas 28 and 29 to compute such a determinant but improve the algorithm by using the fact that $\phi_m(t) \equiv 0 \pmod{p}$ by computing $D_B \bmod \phi_m$ (over $\mathbf{Z}[X]$).

LEMMA 30. *Suppose $D \in \mathbf{Z}[X]$ of degree d and m is a given positive integer, $m < 105$. Let E be the unique element of $\mathbf{Z}[X]$, of degree $< \phi(m)$ such that $E \equiv D \bmod \phi_m$. If $D \in \mathcal{F}_L$ then $E \in \mathcal{F}_K$ for each $K \geq 2^{m-\phi(m)}(d/m + 1)(L - 1) + 1$.*

PROOF. Let $D = \sum_{i=0}^{d} a_i X^i$ and $\delta = \max\{|a_i| : 0 \leq i \leq d\}$. Let $E = \sum_{i=0}^{\phi(m)-1} b_i X^i$ and $\varepsilon = \max_{0 \leq i \leq \phi(m)} |b_i|$. We must show that $2^{m-\phi(m)}(d/m+1)\delta \geq \varepsilon$. We prove this result by induction on d. For $d < \phi(m)$ the result is trivial. Suppose $\phi(m) \leq d < m$ and let $D' = D - a_d X^{d-\phi(m)} \phi_m$, which has degree $< d$. But then $\|D'\|_\infty \leq \delta + |a_d| \, \|\phi_m\|_\infty \leq 2\delta$, as all coefficients of $\phi_m(X)$ are -1, 0 or 1 (for $m < 105$). By repeating this process we find that $\varepsilon \leq 2^{d-\phi(m)+1}\delta$ and the result is proved.

Finally if $d \geq m$ let

$$C = \sum_{j=0}^{m-1} c_j X^j$$

where

$$c_j = \sum_{\substack{i=0 \\ i \equiv j \pmod m}}^{d} a_i.$$

Then $D \equiv C \pmod{X^m - 1}$ and so $D \equiv C \pmod{\phi_m}$ since ϕ_m divides $X^m - 1$. Thus

$$\varepsilon \le 2^{m-\phi(m)} \max_j |c_j| \le 2^{m-\phi(m)}\delta \sum_{\substack{i=0 \\ i \equiv j \pmod m}}^{d} 1 \le \delta \left(\frac{d}{m} + 1\right) 2^{m-\phi(m)}.$$

So, in order to compute the residue of $D_B \bmod \phi_m$ in $\mathbf{Z}[X]$ (for $m < 105$) we use the substitution $X = K$ (with K derived from Lemma 30) and calculate the determinant $\bmod \phi_m(K)$. Now, if $\phi_m(K)$ has many small factors, the computation of this determinant may prove difficult. So, instead, we found a sufficiently large value of K for which $\phi_m(K)$ is prime (using a probabilistic primality test [**26**]).

As we will see in the next section we ran into a surprising problem. For certain values of m and n, every $\phi(n) \times \phi(n)$ submatrix of $\mathbf{A}_n^*$ has zero determinant $\bmod \phi_m$ over $\mathbf{Z}[X]$. In other words, if $\phi_m(t) = 0$ then the matrix $\mathbf{A}_n^*(t)$ has less than full rank (i.e. rank$\le \phi(n) - 1$). This presents a very real problem with the Pollaczek-Morishima method. It means that one can *never* show that $(W_{n,t})$ is true for certain values of n and certain orders of $t \pmod p$. Fortunately in Theorem 4(b) we derived another $4\phi(n)$ rows that we may add to our matrix $\mathbf{A}_n^*$. By using these rows we get a submatrix of full rank over $\mathbf{Z}[X] \pmod{\phi_m}$ and so we can find a nonzero determinant $D \in \mathbf{Z}[X] \pmod{\phi_m}$.

Once we have derived such a nonzero determinant D, it is easy to take $\hat{R}(D, \phi_m)$ and eliminate any prime factors using Wieferich's test.

One final case remains. In §4, we saw that either G has six distinct elements or $G = \{-1, 2, 1/2\}$. In the latter case we only get $3\phi(n)$ equations from Theorem 4(b), and so the case $t \equiv -1 \pmod p$ requires further attention. Here we form the matrix $\mathbf{A}_n^*(-1)$, add the extra $2\phi(n)$ rows to get an integer matrix $\mathbf{I}_n$ (of dimension $4\phi(n) \times \phi(n)$). Then, by computing the Smith normal form of $\mathbf{I}_n$, we derive an integer R such that for all primes p dividing R, $\mathbf{I}_n$ has less than full rank, $\bmod p$. The problem here was that R often turned out to be a very large integer that was extremely hard to factor. With help from Robert Hilchie, Paul VanOorschott, Scott Vanstone and Stephen Watt, who have implemented Lenstra's elliptic curve algorithm [**17**], and from W. Lioen, Robert Silverman, Herman te Riele and D. T. Winter who have implemented the quadratic sieve algorithm [**25a**], we were able to factor the relevant values of R, and then it was a simple matter to apply the Wieferich test.

We finish this section with a summary of the algorithm used to establish $(W_{n+1,t})$ from $(W_{n,t})$ for $t \in H_p^*$.

Procedure to establish $(W_{n+1,t})$ *from* $(W_{n,t})$.

(1) Construct the matrix $\mathbf{A}_n^*$.

(2) Find four subdeterminants of the first $\phi(n) + 3$ rows using Lemma 29; store in $D_1, \ldots, D_4$.

(3) Remove cyclotomic factors and store in S_n.

(4) Apply the Euclidean algorithm in $\mathbf{Z}[X]$ to D_1 and D_2 to find h and R such that p divides R and $h(t) \equiv 0 \pmod{p}$.

(5) Apply the modular Euclidean algorithm in $\mathbf{Z}/R\mathbf{Z}[X]$ to h with D_3 and $D_4 \pmod{R}$ to find new smaller values for h and R.

(6) Divide out small factors ($< 10^5$) from R.

(7) Factor R and apply Wieferich's test to any prime factors found. If we are unable to factor R, we take a different set of $\phi(n) + 3$ rows from $\mathbf{A}_n^*$ and compute another set of four determinants $D_1', \ldots, D_4'$. Then we apply the modular Euclidean algorithm to h with each $D_i' \pmod{R}$ to obtain an integer R', which always has only very small prime factors.

(8) Suppose $\phi_m \in S_n$, $m \neq 1, 2, 3, 4$ or 6. Reduce $\mathbf{A}_n^* \bmod X^m - 1$. Find the maximum K (in Lemma 30) for all subdeterminants of the reduced $\mathbf{A}_n^*$.

(9a) If $\mathbf{A}_n^*$ has full rank $\bmod \phi_m$ then find a submatrix with nonzero determinant D and compute $R = \hat{R}(D, \phi_m)$. Factor R and apply Wieferich's text to each prime factor of R. Go to (10).

(9b) If $\mathbf{A}_n^*$ does not have full rank $\bmod \phi_m$, record (n, m) in Table I. Then add the $4\phi(n)$ extra rows from Theorem 4(b) to $\mathbf{A}_n^*$ and again, by use of Lemma 30, find a submatrix B of nonzero determinant $D_B \pmod{\phi_m}$. Factor $R = \hat{R}(\phi_m, D_B)$ and apply Wieferich's test to each prime factor of R.

(10) For $t = -1$, compute the Smith normal form of $\mathbf{I}_n$. Record any factors $> 10^8$ in Table II and apply Wieferich's test.

10. The results. We checked Pollaczek's computations, which are for the most part correct, with a couple of exceptions—a quite remarkable feat seeing as he had to compute the determinants of up to 12×12 matrices in $\mathbf{Z}[t]$ by hand!

He made the following three mistakes:

His D_{15}' should be multiplied by $t^9/(t^2 - 1)$.

His D_{14} should be multiplied by t^2.

His D_{13}' should read

$$t^{17}(t-1)(t^2-1)^5(t^3-1)(t^4-1)^3(t^6-1)^2(t^7-1)(t^8-1)^2(t^{12}-1)$$
$$\times (t^{20} + 2t^{18} + 10t^{16} + 26t^{14} + 55t^{12} + 40t^{10} + 55t^8 + 26t^6 + 10t^4 + 2t^2 + 1).$$

We now give the three tables that have been discussed previously.

TABLE I

Values of m for which $\mathbf{A}_n^*(t)$ has less than full rank $(\bmod \phi_m(t))$ (for each $n \leq 46$, $m \neq 1, 2, 3, 4$ or 6).

n	m	n	m
14	8	39	7, 14
21	8	41	12
22	12	42	8
26	14	43	12
34	8, 18	44	10
35	8	46	8, 24
38	20		

TABLE II. Factorizations by Lenstra's elliptic curve and quadratic sieve algorithm.

n	Primes p larger than 10^8 for which $\mathbf{I}_n$ has less than full rank $(\mathrm{mod}\, p)$ for each $n \leq 54$.
16	84567933833
20	28126121
22	87389787145802161
24	292743257
26	20744175281242896102 4669
28	60417610459
32	100017905102229761, 183444296565585381 5681 873537110796617190667708837 93
34	251533897238647458557497590 89 180263301094681505688271561866625370036 9
36	2057651004553
38	5954019109, 6406222663, 86856927337, 239971184263 151757932581868856302333
40	28921302541, 158500910993921, 124795802988881
42	6134965909
44	14908207, 230319521501, 3229736074001, 461602566709016523071 68004750241010224814926921329221
46	9714178377707, 337753528260668647654336127148493732714475 6... ...3317229254009957619315256302154730436423560258927177 99
48	227494433, 343402173929, 505614186035085481 184216003478383394808869289600338279 3
50	2041481782091501 485620031213760073713170959369390057221283451799628971692964013981
52	1308435571, 933064021, 5792609881, 6959922191, 20136180968077 764800904013355339 81, 767383453900806874216873841
54	353952504043201218894600827277074935027044702310610366856 73

TABLE III. Factorizations by Pollard's rho algorithm.

For eacn prime $q < 110$, Table III gives those primes $p > 10^6$ for which there exists an integer t such that $t^{q-1} - 1 \equiv (t+1)^{q-1} - 1 \equiv 0 \ (\mathrm{mod}\, p)$ and $t^2 + t + 1 \not\equiv 0 \ (\mathrm{mod}\, p)$

q	p
47	2796203
59	3033169
79	22366891
83	1024099, 1335781, 2135117, 164511353, 370248451, 8831418697
89	2012033, 2236081, 2931542417
97	22253377
101	5827301, 3273601, 8976001
103	2336923, 129159847
107	2965351, 12693077, 17683663, 19617739, 20394401, 26020669 43574057, 52361563, 54087031, 58302757, 79416473, 79953787 209520979, 628616783, 119218851371, 28059810762433
109	5529061

11. The main theorems. By our computations, we may now state the following:

THEOREM 6. *If p is a prime for which Conjecture $2'_p$ is false, then*
(i) *$(W_{n,t})$ is true for $n = 1, 2, \ldots, 46$.*
(ii) *p^2 divides $q^p - q$ for each prime $q \leq 89$.*
(iii) *$p > 714,591,416,091,389$.*

THEOREM 7. *If the First Case of Fermat's Last Theorem is false for prime p then*
(i) *p^2 divides $q^p - q$ for each prime $q \leq 89$, and*
(ii) *$p > 714,591,416,091,389$.*

Theorem 7 follows immediately from Lemma 7 and Theorem 6.

At first glance it might seem that all that has been done is to increase a bound that was already too high to have any real signficance. However the bound itself should only be seen as a corollary to the important result, namely Theorem 7(i). It is to be hoped that, perhaps with some significant increase in our understanding of the behavior of primes, the criteria in Theorem 7(i) will suffice to prove the truth of $(\mathrm{FLTI})_p$ for all primes p. In a heuristic sense one might expect that for a fixed prime q, the probability that p^2 divides $q^p - q$ is $1/p$. If so, then the expected number of primes for which $(\mathrm{FLTI})_p$ is false is less than

$$\sum_{\substack{p > 7.14\times 10^{15} \\ p \text{ prime}}} \frac{1}{p^{24}} \leq \int_{7.14\times 10^{15}}^{\infty} x^{-24}\,dx < 10^{-343}.$$

It might also be hoped that, if $(\mathrm{FLTI})_p$ is false, then we may be able to establish that p^2 divides $q^p - q$ (for a given prime q and $p > p(q)$) without so much explicit computation:

LEMMA 31. *With the notation of* §6 *let $\delta_i = 1 + [k_i/n]$. Then, for each i, $1 \leq i \leq 2\phi(n)$,*

$$\max_{1\leq j\leq \phi(n)} \alpha(k_j, n, k_i) = k_i + 1 - \delta_i \quad \text{and} \quad \min_{1\leq j\leq \phi(n)} \alpha(k_j, n, k_i) = \delta_i.$$

PROOF. Suppose $k_i < n$. If $k_j = n - k_i$ then $\alpha(k_j, n, k_i) = 1 = \delta_i$. Also $\alpha(k_i, n, k_i) = k_i = k_i + 1 - \delta_i$. So now suppose that $k_i > n$. If $\alpha(k_j, n, k_i) = k_i$ then k_i divides k_j, which implies that $k_j \geq k_i > n$, and so $j > \phi(n)$, giving a contradiction. So let $k_j = k_i - n$. Then $\alpha(k_j, n, k_i) = k_i - 1 = k_i + 1 - \delta_i$. If $\alpha(k_j, n, k_i) = 1$ then $k_j \equiv n \pmod{k_i}$, which implies that $k_j > n$, giving a contradiction. So let $k_j = 2n - k_i$. Then $\alpha(k_j, n, k_i) = 2 = \delta_i$.

For each positive integer n let $\mathbf{A}'_n$ be the $2\phi(n) \times \phi(n)$ matrix with (i,j)th entry $X^{\alpha(k_j,n,k_i)-\delta_i}$, where $\delta_i = 1 + [k_i/n]$. It is clear that the ith row of $\mathbf{A}'_n$ is exactly the ith row of $\mathbf{A}_n$ divided by X^{δ_i} and, by Lemma 31, all entries of $\mathbf{A}'_n$ are indeed elements of $\mathbf{Z}[X]$. Also we may re-express Theorem 4(a) as

$$\mathbf{A}'_n(t)\mathbf{W}_n(t) \equiv \mathbf{0} \pmod{p}.$$

Let ϑ_n be the set of all $\phi(n) \times \phi(n)$ subdeterminants of $\mathbf{A}'_n$. By the above, if $\mathbf{W}_n(t) \not\equiv 0 \pmod{p}$ then, for each $B \in \vartheta_n$, we have $B(t) \equiv 0 \pmod{p}$. We make the following conjecture:

CONJECTURE 3_n. *For given positive integer n, if t is a complex number for which $\mathbf{A}'_n(t)$ has* rank $< \phi(n)$, *then either $t = 0$ or t is an mth root of unity for some $m \le 2n$.*

Now suppose that $t^m \not\equiv 1 \pmod p$ for each $m \le 2n$. If Conjecture 3_n holds, then there exist polynomials $f_1, f_2 \in \mathbf{Z}[X]$ (and $B_1, B_2 \in \vartheta_n$ such that each f_i divides B_i) such that $\gcd_{\mathbf{C}[x]}(f_1, f_2) = 1$ and $f_1(t) \equiv f_2(t) \equiv 0 \pmod p$. But then p divides $\hat{R}(f_1, f_2)$, so we may state

LEMMA 32. *Suppose $t \in H_p^*$, $(W_{n,t})$ is true, but $(W_{n+1,t})$ is not true. Suppose also that Conjecture 3_n holds. Then either*

(i) *t has order m $(\le 2n) \pmod p$, or*

(ii) *p divides $\hat{R}(f, g)$ for some $f, g \in \mathbf{Z}[X]$, which are distinct irreducible polynomials dividing some $B_f, B_g \in \vartheta_n$.*

Now by Lemma 15, it is clear that if $p > \alpha^{4n^2/3}$ then Lemma 32(i) cannot hold. We must now try to bound $\hat{R}(f, g)$.

LEMMA 33. *If $B \in \vartheta_n$ then B has degree $d \le 3(n-2)\phi(n)/2$ and $\|B\|_2 \le \phi(n)^{\phi(n)/2}$.*

PROOF. Suppose B is the determinant of submatrix M of $\mathbf{A}'_n$. Now the (i,j)th entry of $\mathbf{A}'_n$ has degree $\alpha(k_j, n, k_i) - \delta_i \le k_i + 1 - 2\delta_i$, by Lemma 31, and so

$$d \le \sum_{i=1}^{\phi(n)} \max_{1 \le j \le \phi(n)} \deg M_{ij}(X)$$
$$\le \sum_{i=\phi(n)+1}^{2\phi(n)} k_i + 1 - 2\delta_i = \frac{3(n-2)\phi(n)}{2}.$$

Now, each entry of M is simply a power of X and so, by Lemma 29, $\|B\|_2 \le \phi(n)^{\phi(n)/2}$.

LEMMA 34. *If $f, g \in \mathbf{Z}[X]$ such that g divides f then $\|g\|_2 \le \alpha^{\deg(f)}\|f\|_2$, where $\alpha = (\sqrt{5}+1)/2$.*

A proof of Lemma 34 may be found in [**9**].

LEMMA 35. *If $f, g \in \mathbf{Z}[X]$ do not have a common root, and divide $B_f, B_g \in \vartheta_n$ (respectively) then*

$$\hat{R}(f, g) \le [\alpha^{3(n-2)}\phi(n)]^{3(n-2)\phi(n)^2/2}.$$

PROOF. Suppose f and g have degrees df, dg respectively. By Lemma 33, df, $dg \le 3(n-2)\phi(n)/2$ and, by Lemmas 33 and 34,

$$\|f\|_2 \le \alpha^{\deg(B_f)}\|B_f\|_2 \le [\alpha^{3(n-2)}\phi(n)]^{\phi(n)/2}.$$

So, by Lemma 20(iv) and (v),

$$\hat{R}(f, g) \le R(f, g) \le \|f\|_2^{dg}\|g\|_2^{df}$$
$$\le \{[\alpha^{3(n-2)}\phi(n)]^{\phi(n)/2}\}^{3(n-2)\phi(n)}.$$

THEOREM 8. *Suppose that Conjecture* 3_m *is true for each* $m \leq n$ *and choose prime* $p > [\alpha^{3(n-2)}(n-1)]^{3(n-2)(n-1)^2/2}$. *If* $(\mathrm{FLTI})_p$ *is false then* p^2 *divides* $q^p - q$ *for each prime* $q \leq 2n+1$.

PROOF. We claim that $(W_{r,t})$ holds for some $t \in G$ and for each $r \leq n+1$. For, by Lemma 15, as $p > \alpha^{4n^2/3}$, there exists $t \in G$ of order $> 2n \pmod p$. So, by Lemma 32, if $(W_{r,t})$ does not hold then p divides $\hat{R}(f,g)$ where f and g divide elements of ϑ_{r-1}. But then by Lemma 35,

$$\begin{aligned} p \leq \hat{R}(f,g) &\leq [\alpha^{3(r-3)}\phi(r-1)]^{3(r-3)\phi(r-1)^2/2} \\ &\leq [\alpha^{3(n-2)}(n-1)]^{3(n-2)(n-1)^2/2} < p, \end{aligned}$$

which gives a contradiction.

Thus $(W_{r,t})$ holds for some $t \in G$ and for each $r \leq n+1$ and, as t has order $> 2n \pmod p$, the result follows from Lemma 18.

We may reword Theorem 8 as follows:

THEOREM 8′. *Suppose Conjecture* 3_n *is true for all integers* n. *If* $(\mathrm{FLTI})_p$ *is false then* p^2 *divides* $q^p - q$ *for each prime* $q \leq \max\{89, 3 + 1.643(\log p)^{1/4}\}$.

PROOF. For $\gamma = 78(\log 53 + 156 \log \alpha)/2809$, it is easy to show that $e^{\gamma(n-1)^4} \geq [\alpha^{3(n-2)}(n-1)]^{3(n-2)(n-1)^2/2}$ for each positive integer $n > 1$. If $q = 2n+1$ then, by Theorem 8, it is clear that p^2 divides $q^p - q$ if $p \geq e^{\gamma(n-1)^4} = e^{\gamma(q-3)^4/16}$. In other words the result holds for $q \leq 3 + \beta(\log p)^{1/4}$ where $\beta = 2/\gamma^{1/4} \sim 1.6431736$.

REMARK. Asymptotically we could take $\gamma = 4.5 \log \alpha$, which would give a value of $\beta \sim 1.6487044$.

ACKNOWLEDGEMENTS. Many people have helped with this paper, by way of providing ideas for the algebra, and computing resources and expertise for the computations. We would particularly like to thank our respective supervisors, Paulo Ribenboim and Gaston Gonnet, for much help and encouragement. Also Jan Minac for his contributions to the algebra, Greg Fee for inputting many ideas for the computations, and Robert Hilchie, W. Lioen, Robert Silverman, Herman te Riele, Paul VanOorschott, Scott Vanstone, Stephen Watt and D. T. Winter for help with the integer factorizations. The first author had a number of useful conversations at the Western Number Theory conference at Asilomar in December 1985, particularly those with Andrew Odlyzko and Hugh Williams.

NOTE ADDED IN PROOF. Tanner and Wagstaff have recently improved upon Sunderson's function $g_n(p)$ (see Lemma 5) and used our Theorem 8′ to show that $(\mathrm{FLTI})_p$ holds for all $p \leq 156,442,236,847,241,650$.

REFERENCES

1. L. M. Adleman and D. R. Heath-Brown, *The first case of Fermat's last theorem*, Invent. Math. **79** (1985), 409–416.
2. E. H. Bareiss, *Silvester's identity and multistep integer preserving Gaussian elimination*, Math. Comp. **22** (1968), 565–578.
3. W. S. Brown, *The subresultant PRS algorithm*, ACM Trans. Math. Software **4** (1978), 237–249.
4. B. W. Char, K. O. Geddes and G. H. Gonnet, *GCDHEU: Heuristic polynomial GCD algorithm based on integer GCD computation*, Proc. Internat. Sympos. Symbolic and Algebraic Manipulation, 1984.
5. L. E. Dickson, *On the last theorem of Fermat*, Quart J. Math. **40** (1908), 27–45.

6. E. Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math. **79** (1985), 383–407.
7. G. Frobenius, *Über den Fermatschen Satz* III, Sitzungsber. Akad. Wiss. Berlin (1914), 653–681.
8. A. J. Goldstein and R. L. Graham, *A Hadamard-type bound on the coefficients of a determinant of polynomials*, Siam Rev. **16** (1974), 394–395.
9. A. J. Granville, *Bounding the two-norm of a divisor of a given polynomial* (to appear).
10. N. G. Gunderson, *Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent*, Thesis, Cornell Univ., 1948.
11. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkorper*, Parts I, Ia, II, J. Deutsch. Math. Verein. **35** (1926), 1–55; **36** (1927), 233–311; supplement, 1930.

11a. D. E. Knuth, *The art of computer programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

12. E. E. Kummer, *Beweis des Fermatschen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$ *für eine unendliche Anzahl Primzahlen* λ, Monatsber. Akad. Wiss., Berlin, 1847, 132–139, 140–141, 305–319.
13. ——, *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall dass die Klassenzahl durch* λ *theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letztes Fermat'schen Lehrsatzes*, Math. Abh. Akad. Wiss., Berlin, 1857, 41–74.
14. A. M. Legendre, *Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat*, Mém. Acad. Sci. Inst. France **6** (1823), 1–60.
15. D. H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. **36** (1981), 289–290.
16. D. H. Lehmer and E. Lehmer, *On the first case of Fermat's last theorem*, Bull. Amer. Math. Soc. **47** (1941), 139–142.
17. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Technical Report #86–18, Math. Inst., Amsterdam, 1986.
18. M. T. McClellan, *The exact solution of systems of linear equations*, J. Assoc. Comput. Mach. **20** (1973), 563–588.
19. M. Mignotte, *Some useful bounds*, Algebra, Symbolic and Algebraic Computation, Springer-Verlag, New York, 1982, pp. 259–263.
20. D. Mirimanoff, *L'équation indéterminée* $x^l + y^l + z^l = 0$ *et le critérium de Kummer*, J. Reine Angew. Math. **128** (1905), 45–68.
21. ——, *Sur le dernier théorème de Fermat*, C.R. Acad. Sci. Paris **150** (1910), 204–206.
22. T. Morishima, *Über die Fermatsche Quotienten*, Japan J. Math. **8** (1931), 159–173.
23. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of F7*, Math. Comp. **29** (1975), 183–205.
24. F. Pollaczek, *Über den grossen Fermat'schen Satz*, Sitzungsber. Akad. Wiss. Wien, Abt. IIa **126** (1917), 45–59.
25. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.

25a. C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory, Math. Centre Tracts 154/155 (H. W. Lenstra, Jr. and R. Tijdeman, eds.), Math. Cent. Amsterdam, 1982, pp. 89–139.

26. M. D. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138.
27. P. Ribenboim, 13 *lectures on Fermat's last theorem*, Springer-Verlag, New York, 1979.
28. J. B. Rosser, *An additional criteria for the first case of Fermat's last theorem*, Bull. Amer. Math. Soc. **47** (1941), 109–110.
29. M. Rothstein, *On pseudo-resultants*, Lecture Notes in Computer Sci., vol. 174, Springer-Verlag, Berlin, 1984.
30. D. Shanks and H. C. Williams, *Gunderson's function in Fermat's last theorem*, Math. Comp. **36** (1981), 291–295.
31. H. S. Vandiver, *Laws of reciprocity and the first case of Fermat's last theorem*, Proc. Nat. Acad. Sci. U.S.A. **11** (1925), 292–298.

32. S. Wagon, *Fermat's last theorem*, Math. Intelligencer **8** (1986), 59–61.
33. S. S. Wagstaff, *The irregular primes to* 125,000, Math. Comp. **32** (1978), 583–591.
34. E. Wendt, *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt dass die Gleichung* $a^n = b^n + c^n$ *fur* $n > 2$, *in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math. **113** (1894), 335–346.
35. A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136** (1909), 293–302.

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO, CANADA K7L 3N6

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA N2L 3G1

Current address (Andrew Granville): Department of Mathematics, University of Toronto, Toronto, Ontario, Canada M5S 1A1

Current address (M. B. Monagan): IBM TJ Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598