The Kummer-Wieferich-Skula Approach to the First Case of Fermat's Last Theorem

Andrew Granville
University of Georgia

Dedicated to Paulo Ribenboim.

1. Introduction.

The First Case of Fermat's Last Theorem is said to be true for prime exponent p if there do not exist integers x, y, z such that

$$x^p + y^p + z^p = 0 \quad \text{where} \quad p \quad \text{does not divide} \quad xyz. \tag{1.1}$$

Instead we shall assume throughout this paper that (1.1) does have solutions and then deduce a variety of implausible consequences.

For example, in 1857 Kummer showed that if (1.1) has a solution then, for all n in the range $2 \leq n \leq p-1$,

$$\text{either} \quad B_{p-n} \equiv 0 \pmod p \quad \text{or} \quad \sum_{j=0}^{p-1} j^{n-1} t^j \equiv 0 \pmod p \tag{1.2}$$

for each $t \in \{-x/y, -y/z, -z/x\}$, where B_n, the nth Bernoulli number, is given by

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

As a consequence one can show that p must divide B_{p-3}, B_{p-5} and many other Bernoulli numbers too.

In 1909 Wieferich surprisingly deduced, from Kummer's criteria, that p^2 must divide $2^p - 2$. Soon others deduced that p^2 must also divide $3^p - 3$, $5^p - 5$ and so on; and Frobenius outlined a method to continue proving such criteria. However it requires a great deal of work to verify each successive

The author is supported, in part, by the National Science Foundation.

criteria, and so, even now, has only been computed up to p^2 divides $q^p - q$, for all $q \leq 89$.

In 1914 Vandiver proved that p divides $B_{p-1}\left(\frac{a}{5}\right) - B_{p-1}$ for $1 \leq a \leq 4$, as well as p^2 divides $5^p - 5$, where $B_{p-1}(t) = \sum_{j=0}^{p-1} \binom{p-1}{j} B_j t^{p-1-j}$ is the $(p-1)$st Bernoulli polynomial. In 1938, Emma Lehmer generalized this to p divides $B_{p-1}\left(\frac{a}{q}\right) - B_{p-1}$ for $1 \leq a \leq q$, for $q = 2, 3, 4$ and 6. Recently Skula showed that one could successively prove that p divides $B_{p-1}\left(\frac{a}{q}\right) - B_{p-1}$ for $1 \leq a \leq q$, for each q, at the same time as proving p^2 divides $q^p - q$.

In this paper we shall present (hopefully easier) proofs of these results, and of some consequences, and give some new results and possible directions.

2. The structure of the pth cyclotomic field and Kummer's Theorem.

Let $\xi = \xi_p$ be a primitive pth root of unity, $K = \mathbf{Q}(\xi)$, and C be the ideal class group of K. Let G be the Galois group of $K \mid \mathbf{Q}$, and χ be a generator of the character group of G (in the multiplicative group of the field of p elements, $\mathbf{F}_p^*$), so that

$$\chi(\sigma_a) = a \quad \text{where} \quad \sigma_a : \xi \mapsto \xi^a.$$

It is well-known (see [Wa], §6.3) that

$$C/C^p = \bigoplus_{i=1}^{p-1} (C/C^p)(\chi^i)$$

where

$$(C/C^p)(\chi^i) = \{I \in C/C^p : I^{\sigma - \chi^i(\sigma)} \in C^p \quad \text{for all} \quad \sigma \in G\};$$

moreover if $i \geq 3$ is odd and $(C/C^p)(\chi^i)$ is non-trivial (contains an element other than C^p) then p divides B_{p-i} (this result is known as Herbrand's Theorem). If we consider the natural homomorphism $\tau : C \mapsto C^p$, defined by $\tau(I) = I^p$, we see that $\ker \tau = \{I : I^P \text{ is principal}\}$. Moreover $C/\ker \tau \cong C^p$ (by the first isomorphism theorem), and so $C/C^p \cong \ker\,\tau$ (as C is an abelian group). Thus we may re-write Herbrand's Theorem to read:

If $i \geq 3$ is odd and

$$(\ker \tau)(\chi^i) := \{I \in C : I^p \text{ and } I^{\sigma - \chi^i(\sigma)} \text{ are principal for all } \sigma \in G\}$$

is non-trivial then p divides B_{p-i}.

One of Kummer's more remarkable ideas was to understand A_p/A_p^p (where A is the ring of integers of K and $A_p = A/pA$) by using logarithmic derivatives (which was later generalized by Coates and Wiles - see §13.7 in [Wa]): For $\gamma = \gamma(\xi) = a_0 + a_1\xi + \ldots + a_{p-1}\xi^{p-1}$, not divisible by $(1-\xi)$, define $\gamma(e^X) = a_0 + a_1e^X + \ldots + a_{p-1}e^{(p-1)X}$ and $\ell_n(\gamma) = \left(\frac{\partial}{\partial X}\right)^n \{\log \gamma(e^X))\} \,|_{X=0}$, for $1 \le n \le p-2$, in $\mathbf{F}_p$ (note that this value is independent of the way that we write γ). Observe that $\ell_n(\gamma(\xi^j)) \equiv j^n \ell_n(\gamma(\xi)) \pmod p$. Kummer noted that $\ell_n(\alpha\beta) \equiv \ell_n(\alpha) + \ell_n(\beta) \pmod p$ and so $\ell_n(\gamma^p) \equiv 0 \pmod p$. Also $\ell_n(\xi^a) = a$ (for $n = 1$), 0 (otherwise), and if $\gamma \in \mathbf{Z}[\xi + \xi^{-1}]$ then $\ell_n(\gamma) \equiv 0 \pmod p$ for odd n in the range $3 \le n \le p-2$: therefore, as every unit u of A is a power of ξ times an element of $\mathbf{Z}[\xi + \xi^{-1}]$ thus $\ell_n(u) = 0$ for odd n in the range $3 \le n \le p-2$. If $(\gamma) = (z)^p$ then $\gamma = uz^p$ for some unit u, and so

$$\ell_n(\gamma) \equiv 0 \pmod p \quad \text{for each odd } \ n, \ 3 \le n \le p-2. \tag{2.1}$$

Let $\eta_i = \sum\limits_{\sigma \in G} \chi^{-i}(\sigma)\sigma$. Observe that if $J = I^{\eta_i}$, for any ideal I, then $J^{\sigma - \chi^i(\sigma)}$ is a power of I^p for every $\sigma \in G$; and so $J \in (\ker \tau)(\chi^i)$ if I^p is principal. Moreover, since $\ell_n(z^{\sigma_a}) \equiv a^n \ell_n(z) \pmod p$ we have

$$\begin{aligned} \ell_n(z^{\eta_i}) &\equiv \sum_{a=1}^{p-1} \chi^{-i}(\sigma_a) a^n \ell_n(z) \\ &\equiv \begin{cases} -\ell_n(z) \pmod p & \text{if } n \equiv i \pmod{p-1}; \\ 0 \pmod p & \text{otherwise.} \end{cases} \end{aligned} \tag{2.2}$$

Now suppose that we have a solution to (1.1). Factoring $x^p + y^p$ we get the ideal equation

$$(x+y)(x+\xi y)\ldots(x+\xi^{p-1}y) = (z)^p.$$

Evidently if $i \not\equiv j \pmod p$ then $(x+\xi^i y, x+\xi^j y)$ divides $(1-\xi)$ (which divides (p)) as $(x,y) = 1$, and so $(x+\xi^i y, x+\xi^j y) = 1$ since p does not divide z. Therefore each $(x+\xi^j y) = I_j^p$ for some ideal I_j, by the unique factorization theorem for ideals. Thus the ideal

$$\theta_i := I^{\eta_i} \ \in (\ker \tau)(\chi^i) \ \text{ for every } 2 \le i \le p-2 \ \text{ (where } I = I_1).$$

If θ_i is non-principal then p divides B_{p-i} by Herbrand's Theorem. On the other hand, if θ_i is principal, say $\theta_i = (z_i)$, then $(z_i)^p = \theta_i^p = I^{p\eta_i} = (x+\xi y)^{\eta_i}$, so that

$$(x+\xi y)^{\eta_i} = u_i \ \text{ in } K^*/(K^*)^p, \tag{2.3}$$

for some unit u_i. Applying $\ell_i(.)$ to both sides of this equation, we deduce from (2.1) and (2.2) that $\ell_i(x+\xi y) \equiv 0 \pmod p$.

This is a 'new' proof of Kummer's result (stated slightly differently), though all the steps presented here are implicit in the literature. However we feel that this proof is more enlightening than the two standard ones, namely that of Kummer (see §7 of [Ri]) which is a mire of complicated details, and that which may be deduced from explicit reciprocity laws (see §9.5 of [Ri]) which is elegant but unilluminating.

Although the statement above is what Kummer actually proved, Mirimanoff simplified it to the statement given in the introduction by observing that, for $t = -y/x$,

$$\ell_n(x+\xi y) = \left(\frac{\partial}{\partial v}\right)^n \{\log(x+e^v y)\}\big|_{v=0} = \left(\frac{\partial}{\partial v}\right)^{n-1} \left\{1 - \frac{1}{1-te^v}\right\} \big|_{v=0}$$

and, as $t \not\equiv 1 \pmod p$ (else p would divide z),

$$\frac{1}{1-te^v} = \frac{1}{1-t^p e^{pv}} \quad \sum_{j=0}^{p-1} t^j e^{jv} \equiv \frac{1}{1-t^p} \sum_{m\geq 0} \left\{ \sum_{j=0}^{p-1} j^m t^j \right\} \frac{v^m}{m!} \pmod p$$

and so

$$\ell_n(x+\xi y) \equiv -\frac{1}{1-t^p} \sum_{j=0}^{p-1} j^{n-1} t^j \pmod p, \quad \text{for all } n \geq 2. \tag{2.4}$$

Pollaczek provided an explicit formula for the polynomials $\ell_n(x+\xi y)$: By noting that

$$\frac{\partial}{\partial v}\left(\frac{1}{1-te^v}\right) = t\frac{\partial}{\partial t}\left(\frac{1}{1-te^v}\right),$$

we deduce that, for $n \geq 2$,

$$\begin{aligned} \ell_n(x+\xi y) &= -\left(\frac{\partial}{\partial v}\right)^{n-1} \frac{1}{1-te^v}\big|_{v=0} \\ &= -\left(\frac{t\partial}{\partial t}\right)^{n-1} \frac{1}{1-te^v}\big|_{v=0} = -\left(\frac{t\partial}{\partial t}\right)^{n-1} \frac{1}{1-t}. \end{aligned}$$

Then, by a straightforward induction hypothesis, we get for $n \geq 2$,

$$\ell_n(x+\xi y) = (-1)^{n+1} \sum_{j=1}^{n} \frac{s_{n,j}}{j} \frac{1}{(t-1)^j}, \tag{2.5}$$

where $s_{n,j}$, the Stirling numbers of the second kind, are defined by $s_{1,j} = 1(\text{for } j=1), 0$ (otherwise), and then $s_{n+1,j} = j(s_{n,j} + s_{n,j-1})$ (so that, for instance, $X^n = \sum_{j=1}^n s_{n,j}\binom{X}{j}$).

It is possible to say a little more above in the case that θ_i is principal: Multiplying (2.3) by its complex conjugate we find that $u_i\overline{u}_i$ is a pth power in K and so, writing $u_i = \xi^a v_i$ for $v_i \in \mathbf{Z}[\xi + \xi^{-1}]$ we find that v_i^2 is a pth power and thus so is v_i. Therefore we can take $u_i = \xi^a$ in (2.3) and comparing $\ell_1(\cdot)$ of both sides gives $a \equiv 0 \pmod p$, and we deduce that $(x+\xi y)^{\eta_i} = 1$ in $K^*/(K^*)^p$. Therefore

$$\prod_{j=1}^{p-1}(x+\xi^j y)^{j^{-i}} = z_i^p \tag{2.6}$$

for some $z_i \in K$. Thaine made this observation some time ago and has since worked to derive a similar criteria for even i, $2 \le i \le p-3$:

3. Thaine's ideas.

Define U_+ to be the group of units of $\mathbf{Z}[\xi + \xi^{-1}]$, which contains the group of 'circular' units, V, generated by $(\xi^a - \xi^{-a})/(\xi - \xi^{-1})$ for $a = 2, 3, \dots, \frac{p-1}{2}$. It is well known that U, the group of units of $\mathbf{Z}[\xi]$, is generated by U_+ together with ξ. It is of great interest to understand the structure of $W = U_+/V$, the non-circular units of $\mathbf{Z}[\xi + \xi^{-1}]$, and particularly its p-part. Again we can decompose

$$W/W^p = \bigoplus_{\substack{i=2\\ i \text{ even}}}^{p-3} (W/W^p)(\chi^i),$$

and a remarkable result of Vandiver tells us that $(W/W^p)(\chi^i)$ is non-trivial if and only if $v_i := \prod_{a=1}^{p-1}\left(\frac{\xi^a - \xi^{-a}}{\xi - \xi^{-1}}\right)^{a^{-i}}$ is a pth power in K (see Theorem 8.14 in [Wa]), say α^p. (Indeed if we define $\theta : W \to W^p$ as $\theta(w) = w^p$ then, proceeding as in the previous section, $W/W^p \cong \ker\theta$, and $\alpha \in (\ker\theta)(\chi^i) = \{w \in W : w^p \text{ and } w^{\sigma - \chi^i(\sigma)} \in V \text{ for all } \sigma \text{ in } G\}$.)

Since

$$\left(\frac{\xi^a - \xi^{-a}}{\xi - \xi^{-1}}\right)^{\eta_i} = v_i^{a^i - 1} \text{ in } V/V^p, \tag{3.1}$$

we can deduce that

$$v^{\eta_i} \text{ is a power of } v_i, \text{ for any } v \in V. \tag{3.2}$$

Moreover, applying (2.2) to (3.1) when a is a primitive root $\pmod p$ (so that $a^i - 1 \not\equiv 0 \pmod p$), we find that $\ell_n(v_i) \equiv 0 \pmod p$ except perhaps when $n = i$, in which case

$$\begin{aligned}
\ell_i(v_i) &\equiv \frac{-1}{a^i-1}\;\ell_i\left(\frac{\xi^a-\xi^{-a}}{\xi-\xi^{-1}}\right) \qquad\qquad \pmod p\\
&= \frac{-1}{a^i-1}\left(\frac{\partial}{\partial v}\right)^i \bigl(\log(e^{2av}-1)-\log(e^{2v}-1)-(a-1)v\bigr)\bigm|_{v=0}\\
&= \frac{-1}{a^i-1}\left(\frac{\partial}{\partial v}\right)^{i-1}\frac{1}{v}\left(\frac{2av}{e^{2av}-1}-\frac{2v}{e^{2v}-1}\right)\bigm|_{v=0} = -\frac{2^i}{i}B_i. \qquad (3.3)
\end{aligned}$$

(Note that if v_i is a pth power then (3.3) implies that p divides B_i.)

Now, assume that $(W/W^p)(\chi^i)$ is trivial. In [Th1], Thaine proved that if $(W/W^p)(\chi^i)$ is trivial then $(C/C^p)(\chi^i)$ is trivial (this may be deduced directly from the 'Main Conjecture', first proved by Mazur and Wiles, but Thaine's proof is much easier, and its generalizations have led to the many recent important advances of Kolyvagin, Rubin and others). This implies that θ_i, from the previous section, must be principal.

Since $(x+\xi y)^{\eta_i} \in \mathbf{Z}[\xi+\xi^{-1}]$ we may assume that $u_i \in U_+$ in (2.3). Therefore $u_i^{\eta_i} \in (W/W^p)(\chi^i)$ (which we have assumed to be trivial), and so $u_i^{\eta_i} \in V$ in U/U^p. But then $u_i^{\eta_i^2} = (u_i^{\eta_i})^{\eta_i}$ is a power of v_i (say, $v_i^{\kappa_i}$) in U/U^p by (3.2). On the other hand, $\eta_i^2 = -\eta_i$ in $\mathbf{F}_p^*$, so that $\eta_i^3 = \eta_i$, and thus raising (2.3) to the power η_i^2 gives us

$$(x+\xi y)^{\eta_i} = v_i^{\kappa_i} \quad \text{in } K^*/(K^*)^p \qquad (3.4)$$

(which is Theorem 2 of [Th2]). Applying $\ell_i(\cdot)$ to both sides gives, by (3.3) and (2.2),

$$\ell_i(x+\xi y) \equiv \kappa_i \frac{2^i}{i} B_i \pmod p \qquad (3.5)$$

Vandiver conjectured that W/W^p is always trivial and this has recently been verified for all $p < 10^6$ in [B]. If this is true but p nonetheless divides B_i then $\ell_i(x+\xi y) \equiv 0 \pmod p$ by (3.3).

Similar arguments also apply in the 'second case' of Fermat's Last Theorem (see [Th2]).

4. p-Divisibility of Bernoulli numbers.

If $t \not\equiv -1, 0$ or $1 \pmod p$ then $\sum_{j=0}^{p-1} j^{3-1} t^j \equiv \frac{t(1+t)}{(1-t)^2}(1-t^p) \not\equiv 0 \pmod p$. Since either $t = -x/y$ or $-y/z$ is $\not\equiv -1, 0$ or $1 \pmod p$, we deduce that p divides B_{p-3} by Kummer's Theorem (1.2). This argument generalizes for if p does not divide B_{p-n} (n odd) then $\sum_{j=0}^{p-1} j^{n-1}t^j \equiv \sum_{j=0}^{p-1} j^{n-1}(1-t)^j \equiv 0 \pmod p$ and so p must divide the resultant of these two polynomials (after dividing them both by appropriate powers of t and $(1-t)$). Krasner showed that this resultant is $< (n-1)!^{2(n-2)}$ (which is $< n^{2n^2}$) and thus $< p$ for $n < (\log p/\log\log p)^{1/2}$. Thus if (1.1) has a solution then p divides B_{p-n} for all $n \le (\log p/\log\log p)^{1/2}$. Explicit computations of this resultant have shown that p must divide B_{p-n} for all $n \le 45$.

Let $\Omega = \{i \ \text{ odd}: \ \ 3 \le i \le p-2 \text{ and } \theta_i \text{ is non-principal}\}$. Then

$$I_k/I_{-k} = \prod_{\substack{i=1 \\ i\ odd}}^{p-1} \theta_i^{-2k^i} = \prod_{\substack{i=1 \\ i\ odd\ \in\Omega}}^{p-1} \theta_i^{-2k^i} \quad \text{in } C$$

(as $\theta_1 \in (\ker \tau)(\chi) \cong (C/C^p)(\chi)$ which is well-known to be trivial–see [Wa], §6.3). Let $r = |\Omega| + 1$. Evidently $\{I_k/I_{-k} : 1 \le k \le r\}$ must be multiplicatively dependent in C, so there exist integers $a_1, \dots, a_r$ such that $\prod_{k=1}^{r} (I_k/I_{-k})^{a_k}$ is principal, and raising this to the pth power we get

$$\prod_{j=1}^{r} \left(\frac{x+\xi^j y}{x+\xi^{-j}y} \right)^{a_j} = uw^p \quad \text{for some } \ w \in K \text{ and unit } u.$$

Multiplying this equation by its conjugate we find that $u\overline{u}$ is a pth power, and so, as in section 2, $u = \xi^b$ for some integer b. So we may write

$$\prod_{j=1}^{r} \left(\frac{1-\xi^j t}{1-\xi^{-j}t} \right)^{a_j} = \xi^b w^p \tag{4.1}$$

where $t = -x/y$. Using (2.4), it is easily verified that

$$\sum_{n=1}^{p-2} \ell_n \left(\prod_{j=1}^{r} \left(\frac{1-\xi^j t}{1-\xi^{-j}t} \right)^{a_j} \right) \left(\sum_{k=1}^{p-1} k^{p-n}\xi^k \right) \equiv \frac{2\sum_{j=1}^{r} ja_j}{1-t^p} + \sum_{j=1}^{r} ja_j \left(\frac{1}{1-\xi^j t} - \frac{1}{1-\xi^{-j}t} \right) \pmod p,$$

and from (4.1) this is $\equiv \sum_{k=1}^{p-1} \xi^k b \equiv -b \pmod p$. Therefore

$$\sum_{j=1}^{r} j a_j \left(\frac{1}{1-\xi^j t} - \frac{1}{1-\xi^{-j} t} \right) \equiv c \pmod p$$

for some integer c. Multiplying through by $\prod_{j=1}^{r}(1-\xi^j t)(1-\xi^{-j}t)$ we see that the coefficient of $\xi^{\frac{p-1}{2}}$ is $0 \pmod p$, and that the coefficient of ξ^i, for some smaller i, is $\not\equiv 0 \pmod p$ (provided $r(r+1) < p-1$) which is impossible. Thus $ii(p) = \#\{2n, 2 \le 2n \le p-3 \text{ and } p \mid B_{2n}\} \ge |\Omega| \ge \sqrt{p} - 2$. (It seems that the proofs in the literature ([Wa], Thm 6.23), usually avoid explicitly using the Kummer homomorphism, but nonetheless take some equivalent logarithmic derivative).

5. p-Divisibility of Fermat quotients.

There does not seem to be any particularly illuminating method of deducing the p-divisibility of Fermat quotients. This is perhaps because they seem to always be expressed as linear combinations of our polynomials $\sum_{j=0}^{p-1} j^{n-1} t^j$, and such combinations only seem to arise naturally in reference to explicit reciprocity laws.

Here we will develop a much shorter version of [GM]: Define $F_t(x) = \frac{1}{1-te^x} = \sum_{n \ge 0} f_n(t) \frac{x^n}{n!}$ so that $f_n(t) = -\ell_{n+1}(1-t\xi) \equiv \frac{1}{(1-t^p)} \sum_{j=0}^{p-1} j^n t^j \pmod p$ by (2.2). From this we see that, for $t \not\equiv 0$ or $1 \pmod p$, $f_{p-1}(t) \equiv 0 \pmod p$. By noting that
$(-1)^{j-1} \cdot \frac{1}{p}\binom{p}{j} = \frac{1-p}{1} \cdot \frac{2-p}{2} \dots \frac{(j-1)-p}{j-1} \cdot \frac{1}{j} \equiv \frac{1}{j} \pmod p$ we see that
$f_{p-2}(t) \equiv \frac{1}{1-t^p} \cdot \left\{ \frac{(t-1)^p - t^p + 1}{p} \right\} \equiv \frac{1}{pz^p}\{x^p + y^p - (x+y)^p\} \pmod p$ for $t = -x/y$. Easy elementary arguments (see §4.3 of [Ri]) give $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod{p^2}$ and $x+y$ is a pth power, so $(x+y)^{p-1} \equiv 1 \pmod{p^2}$; thus $f_{p-2}(t) \equiv 0 \pmod p$. From this and Kummer's congruences (as proved in section 2), we have

$$B_{p-1-n} f_n(t) \equiv 0 \pmod p \tag{5.1}$$

for $n = 1, 2, \dots, p-1$.

In this section we will develop a theory of such congruences by considering the power series of which these functions are coefficients. Thus we rewrite (5.1) as:
For any integers q, r, s,

$$\begin{array}{r} \text{The coefficient of } \; X^{p-1} \; \text{ in } \; B(qX)\{F_t(rX) - F_t(sX)\} \\ \text{is } \; \equiv 0 \pmod p \;\text{ if }\; p \not| \, q \end{array} \tag{5.1$'$}$$

where $B(X) = X/(e^X - 1)$. Incidentally, from the identity

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

we know that

$$\text{(5.2)} \qquad \begin{aligned} &\text{The coefficient of } \ X^{p-2} \ \text{ in } \ F_t(rX)F_t(sX) \\ &\qquad\qquad \text{is } \ \equiv 0 \pmod{p} \ \text{ if } \ p \nmid r-s \end{aligned}$$

(as $f_{p-2}(t) \equiv 0 \pmod{p}$) and so

$$\text{(5.2)}' \qquad f_n(t)f_{p-2-n}(t) \equiv 0 \pmod{p} \quad \text{for} \quad n = 0, 1, 2, \ldots, p-2.$$

There are two other functions, related to $f_{p-2}(t)$ and B_n, which will be of special interest: First, $W_u(t)$, the coefficient of $X^{p-2}/(p-2)!$ in $F_{t,u}(X) = e^{uX}/(1 - te^X)$; proceeding as in the proof of (2.4), we have $W_u(t) \equiv \frac{1}{1-t^p}\sum\limits_{j=0}^{p-1}(j+u)^{p-2}t^j \pmod{p}$. Second, the $(p-1)$st Bernoulli polynomial $B_{p-1}(u)$, the coefficient of $X^{p-1}/(p-1)!$ in $Xe^{uX}/(e^X - 1)$. We also define $C_{m,n}(t) = \frac{1}{m}\sum\limits_{j=0}^{m-1}\left\{B_{p-1}\left(\frac{j}{m}\right) - B_{p-1}\right\}t^{\beta(j,n,m)}$, where $\alpha(a,b,c)$, $\beta(a,b,c)$ are the least positive, non-negative residues of $a/b \pmod{c}$, respectively. Finally let $A_{m,n}(t) := \frac{1}{n}\sum\limits_{j=1}^{n-1} t^{\alpha(j,n,m)}W_{j/n}(t)$.

Our starting point is the identity, for $(m,n) = 1$,

$$\begin{aligned} X\sum_{j=1}^{n-1} t^{\alpha(j,n,m)}F_{t,j/n}(nX) + \sum_{j=0}^{m-1}\frac{X(e^{jX}-1)}{e^{mX}-1}t^{\beta(j,n,m)} + Xt^mF_t(nX) + \\ + \frac{t^m - 1}{m}B(mX)\{F_t(nX) - F_t(0)\} = 0. \end{aligned}$$

Considering the coefficient of $X^{p-1}/(p-1)!$ here, and using (5.1)$'$, we have

$$\text{(5.3)} \qquad C_{m,n}(t) \equiv A_{m,n}(t) \pmod{p}.$$

If $\ell \equiv n \pmod{m}$ then each $\beta(j,\ell,m) = \beta(j,n,m)$ so that $C_{m,\ell}(t) = C_{m,n}(t)$. Moreover if $\ell \equiv -n \pmod{m}$ then $\beta(j,\ell,m) = \beta(m-j,n,m)$ for $1 \le j \le m-1$ and $B_{p-1}\left(\frac{m-j}{m}\right) = B_{p-1}\left(\frac{j}{m}\right)$ (as $B_{p-1}(1-u) = B_{p-1}(u)$ for all u), so that $C_{m,\ell}(t) = C_{m,n}(t)$. We therefore deduce, from (5.3), that

$$\text{(5.3)}' \qquad \text{If } \ m \ \text{ divides } \ \ell \pm n \ \text{ then } \ A_{m,n}(t) \equiv A_{m,\ell}(t) \pmod{p}.$$

Also, if m is an odd prime, then $2\sum\limits_{n=1}^{(m-1)/2} C_{m,n}(t) = \sum\limits_{n=1}^{m-1} C_{m,n}(t)$, which is the coefficient of $X^{p-1}/(p-1)!$ in

$$\frac{1}{m}\sum_{n=1}^{m-1}\sum_{j=0}^{m-1} X\left(\frac{e^{(j/m)X}-1}{e^X-1}\right)\cdot t^{\beta(j,n,m)} = \frac{t^m-t}{t-1}\left(\frac{X/m}{e^{X/m}-1}-\frac{X}{e^X-1}\right)$$

which equals $\frac{t^m-t}{t-1}B_{p-1}(m^{-(p-1)}-1) \equiv \frac{t^m-t}{t-1}\cdot\frac{m^{p-1}-1}{p} \pmod p$ by the Von Staudt-Clausen Theorem. Thus

$$\sum_{\ell=1}^{(m-1)/2} C_{m,\ell}(t) \equiv \frac{t}{2(t-1)}\cdot(t^{m-1}-1)\cdot\frac{m^{p-1}-1}{p} \pmod p. \tag{5.4}$$

So we can now state our induction hypothesis:

$$[W_{n,t}]: \qquad W_{j/\ell}(t)\equiv 0 \pmod p \quad\text{for}\quad 1\le j<\ell\le n-1.$$

Suppose that this holds:

By definition, $A_{m,\ell}(t)\equiv 0 \pmod p$ whenever $1\le\ell\le n-1$ and $(m,\ell)=1$. For any $m, 1\le m\le 2n-1$ with $(m,n)=1$, let $\ell=|n-m|$ so that $(m,\ell)=1$. Then, by (5.3)$'$, $A_{m,n}(t)\equiv A_{m,\ell}(t)\equiv 0 \pmod p$, and so

$$\sum_{\substack{j=1\\(j,n)=1}}^{n-1} t^{\alpha(j,n,m)}W_{j/n}(t)\equiv 0 \pmod p. \tag{5.5}$$

If m is an odd prime then $C_{m,\ell}(t)\equiv 0 \pmod p$ for $1\le\ell\le n-1$ by (5.3), and so

$$(t^{m-1}-1)\cdot\frac{m^{p-1}-1}{p}\equiv 0 \pmod p \tag{5.6}$$

by (5.4). Thus if there exists t satisfying $[W_{n,t}]$ of order $\ge 2n-1$ modulo p, then $m^{p-1}\equiv 1 \pmod{p^2}$ for all primes $m\le 2n-1$.

We would like to be able to deduce $[W_{n+1,t}]$ from $[W_{n,t}]$. This follows from showing that the matrix

$$A_n(t)=\{t^{\alpha(j,n,m)}\}_{\substack{1\le m\le 2n\\1\le j\le n\\(mj,n)=1}}$$

has full rank (i.e. $\phi(n)$) in $\mathbf{F}_p^*$, for then the only solutions to (5.5) come from each $W_{j/n}(t)\equiv 0 \pmod p$. Currently the only known method for doing this is to explicitly compute a few $\phi(n)\times\phi(n)$ subdeterminants and show that they cannot all be simultaneously $0 \pmod p$ (the record is for all $n\le 46$, [GM], where this is all studied in minute detail).

We observe here that if $A_n(t)$ doesn't have full rank over the complex numbers then either $t=0$ or t is an algebraic integer and unit: in particular

t cannot be any rational integer other than $-1, 0$ or 1. To see this look at the square matrix formed by the top $\phi(n)$ rows of $A_n(t)$. The term of lowest (respectively, highest) degree in the mth row is t (t^m), and the furthest such term to the right (left) occurs on the reverse (main) diagonal, that is in column $j = n - m$ ($j = m$). Thus the term of lowest (highest) degree in the determinant of this matrix is $t^{\phi(n)}$ ($t^{n\phi(n)/2}$). So, if $A_n(t)$ does not have full rank then this determinant is 0; by expanding minors we observe that the determinant belongs to $\mathbf{Z}[t]$, and dividing through by $t^{\phi(n)}$ if $t \neq 0$, we see that t is an algebraic integer and a unit (since the polynomial is monic and has last term 1).

6. p-divisibility of Bernoulli polynomials.

(5.3) implies that $C_{m,\ell}(t) \equiv 0 \pmod p$ for $1 \leq \ell \leq n-1$ and any $(m, \ell) = 1$, if $[W_{n,t}]$ holds. We wish to deduce that

$$(6.1) \qquad B_{p-1}\left(\frac{j}{m}\right) - B_{p-1} \equiv 0 \pmod p \quad \text{for all} \quad 1 \leq j \leq m \leq 2n-1,$$

which we shall do by induction on m: So suppose (6.1) holds for all $m' < m$. Then, as $B_{p-1}\left(\frac{m-j}{m}\right) = B_{p-1}\left(\frac{j}{m}\right)$, we have

$$\sum_{\substack{1 \leq j < m/2 \\ (j,m)=1}} (B_{p-1}\left(\frac{j}{m}\right) - B_{p-1})(t^{\beta(j,\ell,m)} + t^{m-\beta(j,\ell,m)}) \equiv 0 \pmod p$$

for each $\ell, 1 \leq \ell < m/2$ with $(\ell, m) = 1$. Thus (6.1) follows for m provided the matrix

$$S_m(t) = \{t^{\beta(j,\ell,m)} + t^{m-\beta(j,\ell,m)}\}_{\substack{1 \leq j,\ell < m/2 \\ (j\ell,m)=1}}$$

has full rank in $\mathbf{F}_p^*$; in other words, non-zero determinant. (Remark: If $[W_{n,1-t}]$ also holds then we can combine $S_m(t)$ and $S_m(1-t)$ to get double as many rows). However, it is easy to show that

$$(6.2) \qquad \det S_m(t) = \prod_{\substack{\chi \text{ an even} \\ \text{character} \pmod m}} \left(\sum_{j=1}^{m} \chi(j) t^j\right).$$

Recently, Dilcher and Skula used this to establish (6.1) for all $m \leq 46$, and Cikánek for $m \leq 94$ with p sufficiently large.

Define the generalized Bernoulli number $B_{n,\chi} = m^{n-1} \sum_{j=1}^{m} \chi(j) B_n\left(\frac{j}{m}\right)$ for characters $\chi \pmod m$. Thus, (6.1) implies that

$$B_{p-1,\chi} \equiv 0 \pmod p \tag{6.3}$$

for all non-principal characters $\chi \pmod m$. Let $L_p(s,\chi)$ be Leopoldt's p-adic L-function. By Theorem 5.11 of [Wa], (6.3) implies that $L_p(2-p,\chi) \equiv 0 \pmod p$, and so, by Corollary 5.13 of [Wa],

$$\begin{aligned} L_p(n,\chi) \equiv 0 \pmod p \quad &\text{for any integer } \ n \ \text{ and even,} \\ &\text{non} - \text{principal character } \ \chi \pmod m. \end{aligned} \tag{6.4}$$

Let u be the least positive residue of $j/m \pmod p$. Then

$$\frac{X(e^{uX}-1)}{e^X-1} = \sum_{n\geq 1} \left(n \sum_{i=0}^{u-1} i^{n-1} \right) \frac{X^n}{n!}, \text{ so that}$$

$$B_{p-1}\left(\frac{j}{m}\right) - B_{p-1} \equiv (p-1) \sum_{1\leq i\leq u-1} \frac{1}{i} \pmod p.$$

$u-1$ runs through $\left[\frac{p}{m}\right], \left[\frac{2p}{m}\right], \dots, \left[\frac{(m-1)p}{m}\right]$ as j runs through $1,2,\dots,m-1$, so that

$$\sum_{1\leq i\leq \left[\frac{jp}{m}\right]} \frac{1}{i} \equiv 0 \pmod p \qquad \text{for } \ 1 \leq j \leq m. \tag{6.5}$$

For each i, $\frac{jp}{m} < i \leq \frac{(j+1)p}{m}$, we consider $k = mi - jp$ in (6.5); thus, for $h \equiv -jp \pmod m$,

$$\sum_{\substack{1\leq k\leq p-1 \\ k\equiv h \pmod m}} \frac{1}{k} \equiv 0 \pmod p \qquad \text{for } \ 0 \leq h \leq m-1. \tag{6.6}$$

Therefore if g is *any* p-integral valued function, of period m, then

$$\sum_{i=1}^{p-1} \frac{g(i)}{i} \equiv 0 \pmod p. \tag{6.7}$$

A particular instance of this is for $g(i) = \xi^i$ for some mth root of unity ξ; giving $f_{p-2}(\xi) \equiv 0 \pmod p$, and so

$$(1-\xi)^p \equiv 1 - \xi^p \pmod{p^2} \quad \text{for each } \ \xi^m = 1. \tag{6.8}$$

Suppose now that m is a prime $\equiv 1 \pmod 4$ and let $\varepsilon = u+v\sqrt{m}$ and $h = h(m)$ be the fundamental unit and class number of $\mathbf{Q}(\sqrt{m})$, respectively. Define $u_n + v_n\sqrt{m} = \varepsilon^n$ and note that

$$\varepsilon^p = (u + v\sqrt{m})^p \equiv u^p + v^p m^{(p-1)/2}\sqrt{m} \equiv u + \left(\frac{m}{p}\right) v\sqrt{m} \bmod p,$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol, so that $\varepsilon^{p-\left(\frac{m}{p}\right)} \equiv \pm 1 \pmod p$. Thus, as is well known, p divides $v_{p-\left(\frac{m}{p}\right)}$, analogous to Fermat's Little Theorem. Now suppose that $\varepsilon^{p-\left(\frac{m}{p}\right)} = \pm 1 + p\omega$ for some $\omega \in \mathbf{Z}[1, \frac{1+\sqrt{m}}{2}]$, so that $\varepsilon^{2h(p-\left(\frac{m}{p}\right))} \equiv 1 \pm 2hp\omega \pmod{p^2}$. On the other hand it is well known that $\varepsilon^{2h} = \prod_{a=1}^{m-1}(1-\xi^a)^{-\left(\frac{a}{m}\right)}$ where ξ is a primitive mth root of unity, and so, by (6.8),

$$\begin{aligned}\varepsilon^{2hp} &= \prod_{a=1}^{m-1}(1-\xi^a)^{-p\left(\frac{a}{m}\right)} \equiv \prod_{a=1}^{m-1}(1-\xi^{ap})^{-\left(\frac{a}{m}\right)} \\ &\equiv \prod_{b=1}^{m-1}(1-\xi^b)^{-\left(\frac{ap^{-1}}{m}\right)} \equiv (\varepsilon^{2h})^{\left(\frac{p}{m}\right)} \pmod{p^2}.\end{aligned}$$

Therefore $\varepsilon^{2h(p-\left(\frac{m}{p}\right))} \equiv 1 \pmod{p^2}$, and by comparing congruences, we find that p divides $2h\omega$. However $h < m$ so that if $m < p$ then p must divide ω and thus

$$p^2 \text{ divides } v_{p-\left(\frac{m}{p}\right)}. \tag{6.9}$$

One expects that this happens very rarely, and for $m = 5$, in which case the v_n are the Fibonacci numbers (see [SS]), it is known that (6.9) fails for all $p < 2^{32}$. In one final observation we note that, by the elementary theory of binary quadratic forms, (6.9) is equivalent to the assertion that

$$h(mp^4) = ph(mp^2) \tag{6.10}$$

where, here, $h(d)$ is the number of equivalence classes of quadratic forms of discriminant d (usually $h(mp^4) = h(mp^2)$ rather than (6.10)).

7. The special case where $x \equiv y$ (mod p).

If the elements of $\{-x/y, -y/z, -z/x, -y/x, -z/y, -x/z\}$ are not distinct $\pmod p$, then evidently they are either all sixth roots of unity (mod p), or they are the set $\{-1, 2, 1/2\}$. The first case here was disposed of by Pollaczek [P] (though his argument needed correcting by Gunderson), while the second remains open. In this section we apply the criteria to this second case. So let $t = 2$.

By (2.5) we find that

$$(-1)^{n+1} f_n(2) = \sum_{j=1}^{n+1} \frac{s_{n+1,j}}{j} = 2 \sum_{j=1}^{n} s_{n,j}.$$

By definition each $s_{n,j}$ is a non-negative integer and $s_{n,1} = 1$ so that $(-1)^{n+1} f_n(2)$ is a positive integer. However since

$$s_{n,j} = j(s_{n-1,j} + s_{n-1,j-1}) \leq n(s_{n-1,j} + s_{n-1,j-1}),$$

we deduce that

$$|f_n(2)| = \sum_{j=1}^{n} s_{n,j} \leq 2n \sum_{j=1}^{n-1} s_{n-1,j} \leq 2n \cdot 2(n-1) \sum_{j=1}^{n-2} s_{n-2,j} \leq \ldots \leq 2^{n-1} n!$$

Thus p does not divide $f_n(2)$ for any $n \leq \log p / \log\log p$, and so, by Kummer's theorem,

$$\text{(7.1)} \qquad B_{p-n} \equiv 0 \pmod{p}, \text{ for all } n \leq \log p / \log\log p.$$

By the final remarks of section 5 we know that the matrix formed by the top $\phi(n)$ rows of $A_n(2)$ has non-zero determinant. Since any entry in the mth row is smaller than 2^m, Hadamard's inequality tells us that this determinant is $< (\phi(n) 2^n)^{\phi(n)/2}$, and since the determinant is an integer, it cannot be divisible by p if $n < \sqrt{\log p}$. Thus $[W_{n,2}]$ holds in this range, and since 2 must have order $> \log p$ modulo p, we deduce from (5.6) that

$$\text{(7.2)} \qquad p^2 \text{ divides } m^p - m \text{ for all } m < 2\sqrt{\log p}.$$

Working in the field of the rationals extended by the primitive $\phi(m)$th roots of unity, we see that $(\det S_m(2))/2^{\phi(m)/2} \equiv 1 \pmod{2}$ (by (6.2)), and so is non-zero. Moreover by the definition of $S_m(2)$ it is clear that its determinant is an integer, and by Hadamard's inequality has absolute value

$$\leq \left(\sum_{a=1,\ (a,m)=1}^{m/2} (2^a + 2^{m-a})^2 \right)^{\phi(m)/4} \leq 2^{m\phi(m)/2}.$$

Thus this cannot be divisible by p if $m < 2\sqrt{\log p}$ and so, by the results of section 6, we know that

$$\text{(7.3)} \quad B_{p-1}\left(\frac{j}{m}\right) - B_{p-1} \equiv 0 \pmod{p} \text{ for all } 1 \leq j \leq m < 2\sqrt{\log p}.$$

Of course all of the equivalent formulations given in section 6, also follow for this range of values of m. (Remark: With a little care, the constant '2' in the '$2\sqrt{\log p}$' above can be improved.)

Collecting these criteria like this, it seems extremely unlikely that such implausible statements can all be simultaneously true, yet we are unable to show that this is the case (even for an infinite sequence of primes).

8. Bernoulli polynomials revisited.

Define

$$C^*_{m,n}(t) = \frac{1}{m} \sum_{\substack{j=0 \\ (j,m)=1}}^{m-1} (B_{p-1}\left(\frac{j}{m}\right) - B_{p-1}) t^{\beta(j,n,m)}.$$

Then

$$\sum_{n=1}^{m-1} \overline{\chi}(n) C^*_{m,n}(t) =$$

$$= \frac{1}{m} \sum_{\substack{j=1 \\ (j,m)=1}}^{m-1} (B_{p-1}\left(\frac{j}{m}\right) - B_{p-1}) \sum_{\substack{n=1 \\ (n,m)=1}}^{m-1} \overline{\chi}(j)\chi(j/n) t^{\beta(j,n,m)}$$

$$\equiv B_{p-1,\overline{\chi}} \left(\sum_{\substack{r=1 \\ (r,m)=1}}^{m} \chi(r) t^r \right) \pmod p$$

if χ is non-principal. (Note that $C^*_{m,n}(t) = \sum_{d|m} \frac{\mu(d)}{d} C_{m/d,n}(t^d)$).

Now suppose that m is prime so that $C^*_{m,n}(t) = C_{m,n}(t)$. From $[W_{n,t}]$ we obtain that, for even character $\chi \pmod m$,

$$B_{p-1,\chi} \cdot \left(\sum_{r=0}^{m-1} \overline{\chi}(r) t^r \right) \equiv 0 \pmod p, \tag{8.1}$$

where $B_{p-1,\chi_0} = \frac{m^{p-1}-1}{p}$ by our (new) definition.

Evidently there exists a prime ideal $\mathbf{p}$ dividing p in $\mathbf{Q}(\xi_{m-1})$, and a character $\chi \pmod m$, such that

$$\mathbf{p} \text{ divides } B_{p-1,\chi} \tag{8.2}$$

for, if not, each $\sum_{r=1}^{m-1} \overline{\chi}(r) t^r \equiv 0 \pmod p$ and so

$$0 \equiv \sum_{\chi \ even} \chi(s) \sum_{r=0}^{m-1} \overline{\chi}(r) t^r \equiv \frac{m-1}{2} \cdot (t^s + t^{m-s}) \pmod p$$

which is impossible for $s = \frac{m-1}{2}$, $t \not\equiv 0$ or $-1 \pmod p$.

By Iwasawa's *Main Conjecture*, proved by Coates and Wiles, we can deduce from (8.2) that

$$(C/C^p)^{\frac{1}{\phi(n)(p-1)}\sum_{a=1}^{mp}\left(\sum_{\tau\in \mathrm{Aut}(\mathbf{Q}(\chi)/\mathbf{Q})}(\tau\chi)(a)a\sigma_a^{-1}\right)} \tag{8.3}$$

is non-trivial, where C is now the ideal class group of $\mathbf{Q}(\xi_{np})$. It seems to me to be extremely likely that one should be able to explicitly identify some element of this component (like in section 2), though I have thus far been unable to do so. If one did, it would surely lead to a new approach to proving results like those in the last four sections, and perhaps a much better understanding as to why they hold.

9. A curve with many $\mathbf{F}_p^2$-points.

Let g be a primitive root modulo p, and define $\log_p j$ to be that integer (modulo $p-1$) for which $g^{\log_p j} \equiv j \pmod p$. Define

$$G_p(X,Y) = \sum_{j=1}^{p-1} X^{\log_p j} Y^j,$$

so that

$$G_p(g^n,t) \equiv \sum_{j=1}^{p-1} j^n t^j \equiv (1-t^p) f_n(t) \pmod p,$$

and thus if (1.1) has solutions then, by (5.2)$'$,

$$G_p(g^n,t)G_p(g^{p-2-n},t) \equiv 0 \pmod p \quad \text{for } n = 0,1,2,\dots,p-2. \tag{9.1}$$

This will usually lead to at least $3(p-1)$ non-trivial zeros of the curve $G_p(x,y) = 0$ in $\mathbf{F}_p^2$. Generally we expect a curve to have around p such zeroes, and very rarely as many as $3(p-1)$. This is true of $G_p(x,y) = 0$ for the primes $p < 1000$. Unfortunately we are unable to use Weil's Theorem to *prove* something of this sort since there one needs a curve of low genus ($< \sqrt{p}$), while $G_p(x,y) = 0$ seems to have high genus (order p^2).

10. Our matrices revisited.

It seems to be difficult to prove that $A_n(t)$ has full rank directly. (If we could do so then one could deduce that p^2 divides $m^p - m$ for all

$m < (\log p)^{1/4}$ — see [GM].) However the following generalization seems worth pursuing:

Let $A(X)$ be an m-by-n matrix (with $m \geq n$), in which each entry is a power of X, and suppose that every n-by-n submatrix of $A(X)$ has non-zero determinant. We conjecture that there is some function $m(n)$ such that if $n \geq m(n)$ and $A(t)$ does not have full rank then either t is 0 or a root of unity. Perhaps we can even take $m(n) = 2n$.

Van der Poorten and I observed that if $m \geq n(n^2 - 2n + 3)/2$ and $A(t)$ has rank $r < n$ then either t is 0 or an algebraic unit. We will prove this assuming also that t is an algebraic integer – the necessary modifications for arbitrary algebraic t are minor: If t is not a unit then select an r-by-$(r+1)$ submatrix $B(X)$ of $A(X)$, such that $B(t)$ has rank r (which exists since $A(t)$ has rank r). Let $p_j(X)$ be the determinant of the r-by-r minor formed by deleting the jth column of $B(X)$ – at least one $p_j(X)$ must be non-zero else $B(t)$ would have rank $< r$. Now if $(X^{a_1}, \dots, X^{a_{r+1}})$ are the entries (in the same columns as in $B(X)$) of any other row of $A(X)$ then the determinant of the matrix formed by adjoining this new row to $B(X)$ is

$$X^{a_1}p_1(X) - X^{a_2}p_2(X) \dots \pm X^{a_{r+1}}p_{r+1}(X). \tag{10.1}$$

Let $(t)^{\pi_j}$ be the largest power of the ideal (t) that divides $p_j(t)$, and define Q to be the smallest $a_j + \pi_j$. Since the sum in (10.1) with $X = t$ equals 0, we examine this sum modulo $(t)^{Q+1}$ and observe that there must be integers $i \neq j$ such that $a_i + \pi_i = Q = a_j + \pi_j$. Since there are $\binom{n}{2}$ possible pairs (i, j), some such pair must occur here at least n times since we have $m - (n-1) > \binom{n}{2}(n-1)$ possibilities for the row that we adjoined to $B(X)$. But in the matrix M formed by n such rows we see that X^{π_i} times the ith column equals X^{π_j} times the jth column, and thus M does not have full rank, contradicting the hypothesis.

Acknowledgements: Much of my interest and understanding in this topic evolved during the enjoyable period in which I was a doctoral student under Paulo Ribenboim — thank you. This paper also benefitted from discussions and/or correspondance with Enrico Bombieri, Karl Dilcher, Ladja Skula, Zhi-Wei Sun and Alf Van der Poorten, as well as the excellent referee — thanks to you all.

References

[B] Buhler, J.P., Crandall, R.E. and Sompolski, R.W., *Irregular primes to one million*, (preprint).

[Fr] Frobenius, G., *Über den Fermatschen Satz* III, Sitzungsber. Adad. Wiss. Berlin (1914), 653-681.

[GM] Granville, A. and Monagan, M. B., *The First Case of Fermat's Last Theorem is True for all Prime Exponents up to 714,591,416,091,389*, Trans. A.M.S., **306** (1988), 329-359.

[Ku] Kummer, E. E., *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.

[Le] Lehmer, E., *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Annals of Math., **39** (1938), 350-359.

[P] Pollaczek, F., *Über den grossen Fermat'schen Satz*, Sitzungsber. Akad. d. Wiss. Wien IIa, **126** (1917), 45-59.

[Ri] Ribenboim, P., 13 *Lectures on Fermat's last theorem*, (Springer-Verlag, New York, 1979).

[Sk] Skula, L., *Fermat's Last Theorem and the Fermat quotients*, Comm. Math. Univ. Sancti Pauli, **41** (1992), 35-54.

[SS] Sun, Z.-H. and Sun, Z.-W., *Fibonacci numbers and Fermat's Last Theorem*, Acta Arithm., **60** (1992), 371-388.

[Th1] Thaine, F., *On the ideal class groups of real abelian number fields*, Annals of Math., **128** (1988), 1-18.

[Th2] Thaine, F., *On Fermat's Last Theorem and the Arithmetic of* $\mathbf{Z}[\xi_p + \xi_p^{-1}]$, J. of Number Theory, **29** (1988), 297-299.

[Wa] Washington, L.C., *Introduction to Cyclotomic Fields*, Grad. Text in Math. 83, (Springer-Verlag, New York, 1982).

[Wi] Wieferich, A., *Zum letzten Fermat'schen Satz*, J. Reine Angew. Math. **136** (1909), 293-302.

Andrew Granville
Department of Mathematics
University of Georgia
Athens, GA 30602
USA
e-mail andrew@sophie.math.uga.edu