Class field theory and the first case of Fermat's last theorem

H. W. Lenstra, Jr. and P. Stevenhagen

For a prime number p, the *first case* of Fermat's last theorem for exponent p asserts that for any three integers x, y, z with $x^p + y^p + z^p = 0$, at least one of x, y, z is divisible by p. In the present chapter we use class field theory to prove several classical results concerning the first case. Our treatment is based on Hasse's exposition [6, Section 22], but whereas Hasse applied explicit reciprocity laws, our proofs depend only on general properties of power and norm residue symbols.

Theorem 1. *The first case of Fermat's last theorem with exponent p is correct for each prime number p for which $2p + 1$ is prime.*

This theorem is due to Sophie Germain (1823).

For a positive integer k, we define $N_k = \prod_{\eta,\vartheta}(1 + \eta + \vartheta)$, the product ranging over all kth roots of unity η and ϑ in an algebraic closure of the field $\mathbf{Q}$ of rational numbers. It is easy to see that N_k is a rational integer for each k, and that N_k vanishes if and only if k is divisible by 3.

Theorem 2. *Let p be a prime number, and suppose that there exists a positive integer k not divisible by p for which $kp + 1$ is a prime number not dividing N_k. Then the first case of Fermat's last theorem with exponent p is correct.*

This result, which is similar to a theorem of Wendt (1894), is taken from [1]. The integer k is necessarily even and not divisible by 3.

Let k be a positive integer, and let T_k be the set of odd primes p for which p divides k or $kp + 1$ is a prime factor of N_k. By Theorem 2, the first case of Fermat's last theorem is correct for exponent p if p is a prime number not in T_k for which $kp + 1$ is prime. When k is not divisible by 3, the estimate $|N_k| \leq 3^{k^2}$ shows that the exceptional set T_k has cardinality at most $k^2 + \log k$.

In 1985, Adleman, Heath-Brown, and Fouvry [1, 4] deduced from Theorem 2 that the first case is valid for infinitely many p, as follows. Using sieve methods, Fouvry showed that there exists $c > 0$ with the following property: for all sufficiently large t, there are at least $c \cdot t/\log t$ prime numbers $q \leq t$ with $q \equiv 2 \bmod 3$ for which $q - 1$ has a prime factor $p > t^{0.6687}$. Each pair q, p gives rise to an integer $k = (q-1)/p$ that is less than $u = t^{0.3313}$. The inequality $c \cdot t/\log t > u \cdot (u^2 + \log u)$, which is valid when t is large enough, shows that some value of k must arise for more than $k^2 + \log k$ pairs q, p. For at least one of these pairs the number p is outside T_k, so that the first case holds for p.

From $N_2 = -3$ one finds that T_2 is empty, so Theorem 1 follows from Theorem 2, with $k = 2$. In general, when k is a given positive integer that is not divisible by 3, then it is usually easy to deduce from Theorem 2 that the first case of Fermat's last theorem is correct for each prime exponent p for which $kp+1$ is prime. For example, from

$$N_4 = -3 \cdot 5^3, \qquad N_8 = -3^7 \cdot 5^3 \cdot 17^3, \qquad N_{10} = -3 \cdot 11^9 \cdot 31^3$$

one finds $T_4 = T_8 = \emptyset$ and $T_{10} = \{3, 5\}$. Since Theorem 1 applies to $p = 3$ and to $p = 5$, one concludes that the first case is true for p if $4p+1$, $8p+1$, or $10p+1$ is a prime number. This result is due to Legendre (1823). Exceptional primes p that may arise for other values of k are generally easily dealt with by means of the following theorem.

Theorem 3. *Let p be a prime number, and suppose that the first case of Fermat's last theorem for exponent p is false. Then we have*
(a) $2^{p-1} \equiv 1 \bmod p^2$,
(b) $3^{p-1} \equiv 1 \bmod p^2$.

These two results are due to Wieferich (1909) and Mirimanoff (1910), respectively.

There is an efficient algorithm that for a given prime number p tests the validity of (a) and (b). It is believed that there is not a single prime p satisfying both (a) and (b), so that this algorithm, combined with Theorem 3, could be used to prove the first case of Fermat's last theorem for any given prime exponent. This belief is borne out by numerical experiments. In fact, of all primes for which (a) has ever been tested—and this includes all primes less than $4 \cdot 10^{12}$ (see [3])—only $p = 1093$ and $p = 3511$ satisfy (a), and neither of these primes satisfies (b). (The only primes $p < 2^{32} \approx 4.3 \cdot 10^9$ satisfying (b) are $p = 11$ and $p = 1{,}006{,}003$, see [8].)

It is an amusing consequence of (a) that the first case of Fermat's last theorem holds for exponents that are Mersenne or Fermat primes.

Several mathematicians proved, with the same hypotheses as in Theorem 3, that for various other small prime numbers q one has $q^{p-1} \equiv 1 \bmod p^2$. The best result of this nature, prior to the work of Wiles and Taylor, was obtained by Granville and Monagan [5], who covered all prime numbers $q \leq 89$. If it had been possible to replace 89 by an expression that tends sufficiently rapidly to infinity with p, such as $4 \cdot (\log p)^2$, then the first case of Fermat's last theorem would have followed for all p, by [7]; but this could apparently not be achieved by the method of [5]. However, by a theorem of Gunderson (1948) the bound 89 is good enough to imply the first case for all p up to the limit in the title of [5]. Tanner and Wagstaff [9] improved upon Gunderson's work and raised the limit to 156,442,236,847,241,729.

In the proofs, we let p be a prime number, and we let ζ be a primitive pth root of unity in an extension field of $\mathbf{Q}$. We denote by $(-)$ the pth power residue symbol for the cyclotomic field $\mathbf{Q}(\zeta)$, and by $\mathfrak{p} = (\zeta - 1)$ the unique prime of $\mathbf{Q}(\zeta)$ lying over p. The properties of power and norm residue symbols that we use can all be found in [2, pp. 348–353].

Let it now be supposed that x, y, z are integers not divisible by p that satisfy $x^p + y^p + z^p = 0$. Clearly, p is odd. Removing a greatest common divisor, we may assume that x, y, z are pairwise coprime. We have $\prod_{i=0}^{p-1}(x + y\zeta^i) = x^p + y^p = -z^p$, and from $\gcd(x, y) = \gcd(p, z) = 1$ it follows that the factors $x + y\zeta^i$ are pairwise coprime. Hence each factor generates an ideal that is a pth ideal power.

Lemma 1. *Let n be an integer that is coprime to p and z. Then we have $\left(\frac{x+y\zeta}{n}\right) = \left(\frac{\zeta}{n}\right)^{-y/z}$, where the exponent $-y/z$ is computed modulo p.*

Proof. With $\alpha = (x + y\zeta)\zeta^{y/z}$, the assertion reads $\left(\frac{\alpha}{n}\right) = 1$. Note that (α) is a pth ideal power that is coprime to n, so the definition of the power residue symbol gives $\left(\frac{n}{\alpha}\right) = 1$. The general power reciprocity law (see [2, p. 352, Exercise 2.10]) asserts in this case that $\left(\frac{\alpha}{n}\right)\left(\frac{n}{\alpha}\right)^{-1}$ equals the $\mathfrak{p}$-adic pth power norm residue symbol $(n, \alpha)_{\mathfrak{p}}$. Hence it suffices to prove $(n, \alpha)_{\mathfrak{p}} = 1$. We do this by a computation in the ring of integers of the local field at $\mathfrak{p}$. The units of that ring taken modulo $\mathfrak{p}^2$ are of the form $a + b(\zeta - 1)$, where a, $b \in \mathbf{Z}/p\mathbf{Z}$, $a \neq 0$. They form a group of order $(p-1)p$, which is the direct product of a group of order $p - 1$, consisting of the elements with $b = 0$, and a group of order p, consisting of the elements with $a = 1$; the latter group is generated by ζ, since $\zeta^b \equiv 1 + b(\zeta - 1) \bmod (\zeta - 1)^2$. A general element $a + b(\zeta - 1)$ is decomposed as $a \cdot \zeta^{b/a}$. Applying this to $x + y\zeta \pmod{\mathfrak{p}^2}$, which has $a = x + y \equiv -z \bmod p$ and $b = y$, we find that the $\langle\zeta\rangle$-component of $x + y\zeta \pmod{\mathfrak{p}^2}$ equals $\zeta^{-y/z}$. The other component must then be $(x + y\zeta)/\zeta^{-y/z} = \alpha$. Therefore the order of $\alpha \pmod{\mathfrak{p}^2}$ divides $p - 1$, and $\alpha^{p-1} = 1 - \beta$ with $\beta \in \mathfrak{p}^2$. Also, n^{p-1} is of the form $1 - \gamma$, with $\gamma \in (p) = \mathfrak{p}^{p-1}$. From $\beta\gamma \in \mathfrak{p}^{p+1}$ it follows that $1 - \beta\gamma = \delta^p$ for some non-zero δ in the $\mathfrak{p}$-adic field (cf. [2, p. 353, Exercise 2.12]). Using the bimultiplicativity of the norm residue symbol and the fact that $(1 - \gamma, \gamma)_{\mathfrak{p}} = 1$ we find

$$(n, \alpha)_{\mathfrak{p}} = (n^{p-1}, \alpha^{p-1})_{\mathfrak{p}} = (1 - \gamma, 1 - \beta)_{\mathfrak{p}} = (1 - \gamma, (1 - \beta)\gamma)_{\mathfrak{p}} = 1,$$

the last step because $(1 - \gamma) + (1 - \beta)\gamma = \delta^p$ (see [2, p. 351, Exercise 2.5]). This proves Lemma 1.

From Lemma 1, we obtain the following result of Furtwängler (1912).

Lemma 2. *We have $q^{p-1} \equiv 1 \bmod p^2$ for every prime number q that satisfies one of the following conditions:*

(i) *q divides x, y, or z;*

(ii) *one of the differences $x - y$, $y - z$, $z - x$ is divisible by q but not by p.*

Proof. Suppose first that q is a prime number dividing y. Then q does not divide p or z, so we can apply Lemma 1 with $n = q$ to find $\left(\frac{x}{q}\right) = \left(\frac{x+y\zeta}{q}\right) = \left(\frac{\zeta}{q}\right)^{-y/z}$. As $\left(\frac{x}{q}\right)$ is a Galois-invariant pth root of unity, it equals 1. Also $-y/z \not\equiv 0 \bmod p$, so we have $\left(\frac{\zeta}{q}\right) = 1$. The formula $\left(\frac{\zeta}{q}\right) = \zeta^{(q^{p-1}-1)/p}$ from [2, p. 349, Exercise 1.6] now implies $q^{p-1} \equiv 1 \bmod p^2$.

Next, suppose that q is a prime number dividing $x-y$, and that $x-y$ is not divisible by p. Clearly, we may assume that q does not divide z. From the equality $\left(\frac{x+y\zeta}{q}\right) = \left(\frac{y+x\zeta}{q}\right)$ it follows, by another application of Lemma 1, that $\left(\frac{\zeta}{q}\right)^{-y/z}$ and $\left(\frac{\zeta}{q}\right)^{-x/z}$ are equal. As $-y/z$ and $-x/z$ are not congruent modulo p, this implies $\left(\frac{\zeta}{q}\right) = 1$. As before, we obtain $q^{p-1} \equiv 1 \bmod p^2$. This proves Lemma 2.

We derive Theorem 3 from Lemma 2. By the assumption of the theorem, there exist x, y, z as above. As one of x, y, z is even, condition (i) holds for $q=2$. This yields (a). To prove (b), we first note that by (a) we have $p \neq 3$. It suffices to show that one of the conditions in Lemma 2 is met by $q=3$. If 3 divides one of x, y, z, then (i) holds. Otherwise, the congruence $x^p + y^p + z^p \equiv 0 \bmod 3$ shows that 3 divides all differences $x-y$, $y-z$, $z-x$; but from $3x^p \not\equiv 0 \bmod p$ it follows that these differences are not all divisible by p, so (ii) holds. This completes the proof of Theorem 3.

We next prove Theorem 2. Let k be a positive integer for which $q = kp+1$ is prime. It suffices to show that if x, y, z are as above, then p divides k or q divides N_k. We distinguish two cases. First suppose that one of x, y, z is divisible by q. From Lemma 2 it follows that $q^{p-1} \equiv 1 \bmod p^2$, so we have $1 + kp = q \equiv q^p = (1+kp)^p \equiv 1 \bmod p^2$. Thus, in this case p divides k. Next, suppose that none of x, y, z is divisible by q. From $p = (q-1)/k$ we see that each of x^p, y^p, z^p, when taken modulo q, is a kth root of unity in the finite field $\mathbf{Z}/q\mathbf{Z}$. Hence there are, in the ring of q-adic integers, kth roots of unity ϵ, $\epsilon\eta$, $\epsilon\vartheta$ (say) that are congruent to x^p, y^p, and z^p, respectively, modulo q. From $x^p + y^p + z^p = 0$ we find $1 + \eta + \vartheta \equiv 0 \bmod q$, so that now q divides N_k. This proves Theorem 2.

Above we saw already that Theorem 1 follows from Theorem 2.

References

1. L.M. Adleman, D.R. Heath-Brown, *The first case of Fermat's last theorem*, Invent. math. **79** (1985), 409–416.
2. J.W.S. Cassels, A. Fröhlich (eds), *Algebraic number theory, Proceedings of an Instructional Conference*, Academic Press, 1967.
3. R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., to appear.
4. E. Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. math. **79** (1985), 383–407.
5. A. Granville, M.B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714,591,416,091,389, Trans. Amer. Math. Soc. **306** (1988), 329–359.
6. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz*, Jber. Deutsch. Math.-Verein. Ergänzungsband **6** (1930), 1–204.
7. H.W. Lenstra, Jr., *Miller's primality test*, Inform. Process. Lett. **8** (1979), 86–88.
8. P. Montgomery, *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. **61** (1993), 361–363.
9. J.W. Tanner, S.S. Wagstaff, Jr., *New bound for the first case of Fermat's last theorem*, Math. Comp. **53** (1989), 743–750.

Acknowledgment.

The assistance of Andrew Granville and Wilfrid Keller is gratefully acknowledged. The first author was supported by NSF grant No. DMS–9224205.

Department of Mathematics # 3840
University of California
Berkeley, CA 94720–3840
U.S.A.

Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands

Appendix

H. W. Lenstra, Jr. and P. Stevenhagen

Theorem. *Let p be a prime number, and suppose that x, y, z are pairwise coprime integers not divisible by p for which $x^p + y^p + z^p = 0$. Then we have*
(a) $2p + 1$ *is composite,*
(b) $2^{p-1} \equiv 1 \bmod p^2$,
(c) $3^{p-1} \equiv 1 \bmod p^2$,
(d) $q^{p-1} \equiv 1 \bmod p^2$ *for each prime number q dividing xyz.*

The assertions of the theorem are due to Sophie Germain (1823), Wieferich (1909), Mirimanov (1910), and Furtwängler (1912), respectively. Hasse [2, sec. 22] derived these results from the explicit reciprocity laws of class field theory. Below we give a simplified version of his proof. It depends only on general properties of power and norm residue symbols, as can be found in [1, pp. 348–353].

Let p, x, y, z be as in the theorem. Clearly, p is odd. We denote by ζ a primitive pth root of unity in an extension field of the field $\mathbf{Q}$ of rational numbers, by $\left(\frac{-}{-}\right)$ the pth power residue symbol for the cyclotomic field $\mathbf{Q}(\zeta)$, and by $\mathfrak{p} = (\zeta - 1)$ the unique prime of the same field lying over p.

We have $\prod_{i=0}^{p-1}(x + y\zeta^i) = x^p + y^p = -z^p$, and from $\gcd(x, y) = \gcd(p, z) = 1$ it follows that the p factors $x + y\zeta^i$ are pairwise coprime. Hence each factor generates an ideal that is a pth ideal power.

Lemma. *For any prime number q not dividing pz we have $\left(\frac{x+y\zeta}{q}\right) = \left(\frac{\zeta}{q}\right)^{-y/z}$, where the exponent $-y/z$ is computed modulo p.*

Proof. With $\alpha = (x + y\zeta)\zeta^{y/z}$, the lemma asserts that $\left(\frac{\alpha}{q}\right) = 1$. Note that (α) is a pth ideal power that is coprime to q, so the definition of the power residue symbol gives $\left(\frac{q}{\alpha}\right) = 1$. The general power reciprocity law (see [1, p. 352, Exercise 2.10]) asserts in this case that $\left(\frac{\alpha}{q}\right)\left(\frac{q}{\alpha}\right)^{-1}$ equals the $\mathfrak{p}$-adic pth power norm residue symbol $(q, \alpha)_{\mathfrak{p}}$. Hence it suffices to show that the latter symbol equals 1. We do this by a computation in the ring of integers of the local field at $\mathfrak{p}$. The units of that ring taken modulo $\mathfrak{p}^2$ are of the form $a + b(\zeta - 1)$, where a, $b \in \mathbf{Z}/p\mathbf{Z}$, $a \neq 0$. They form a group of order $(p-1)p$, which is the direct product of a group of order $p - 1$, consisting of the elements with $b = 0$, and a group of order p, consisting of the elements with $a = 1$; the latter group is generated by ζ, since $\zeta^b \equiv 1 + b(\zeta - 1) \bmod (\zeta - 1)^2$. A general element $a + b(\zeta - 1)$ is decomposed as $a \cdot \zeta^{b/a}$. Applying this to $x + y\zeta \pmod{\mathfrak{p}^2}$, which has $a = x + y \equiv -z \bmod p$, $b = y$, we find that the $\langle\zeta\rangle$-component of $x + y\zeta \pmod{\mathfrak{p}^2}$ equals $\zeta^{-y/z}$. The other component must then be

$(x+y\zeta)/\zeta^{-y/z} = \alpha$. Therefore the order of $\alpha \pmod{\mathfrak{p}^2}$ divides $p-1$, and $\alpha^{p-1} = 1-\beta$ with $\beta \in \mathfrak{p}^2$. Also, q^{p-1} is of the form $1-\gamma$, with $\gamma \in (p) = \mathfrak{p}^{p-1}$. From $\beta\gamma \in \mathfrak{p}^{p+1}$ it follows that $1-\beta\gamma = \delta^p$ for some non-zero δ in the $\mathfrak{p}$-adic field (cf. [1, p. 353, Exercise 2.12]). Using the bimultiplicativity of the norm residue symbol and the fact that $(1-\gamma,\gamma)_{\mathfrak{p}} = 1$ we find that

$$(q,\alpha)_{\mathfrak{p}} = (q^{p-1},\alpha^{p-1})_{\mathfrak{p}} = (1-\gamma,1-\beta)_{\mathfrak{p}} = (1-\gamma,(1-\beta)\gamma)_{\mathfrak{p}} = 1,$$

the last step because $(1-\gamma)+(1-\beta)\gamma = \delta^p$ (see [1, p. 351, Exercise 2.5]). This proves the lemma.

We prove part (d) of the theorem. Let q be a prime number dividing y. From the lemma we find that $\left(\frac{x}{q}\right) = \left(\frac{x+y\zeta}{q}\right) = \left(\frac{\zeta}{q}\right)^{-y/z}$. But $\left(\frac{x}{q}\right)$ is a Galois-invariant pth root of unity, so it equals 1. Also $-y/z \not\equiv 0 \bmod p$, so we find that $\left(\frac{\zeta}{q}\right) = 1$. From [1, p. 349, Exercise 1.6] we see that $\left(\frac{\zeta}{q}\right) = \zeta^{(q^{p-1}-1)/p}$. Therefore we have $q^{p-1} \equiv 1 \bmod p^2$, which implies (d).

Clearly xyz is even, so with $q=2$ we obtain (b).

To prove (a), suppose that $q = 2p+1$ is prime. Then $p = (q-1)/2$, so each of x^p, y^p, z^p is congruent to 0, 1, or -1 modulo q. Since their sum is 0 modulo q, and $q > 3$, at least one is 0 mod q. Hence by (d) we have $q^{p-1} \equiv 1 \bmod p^2$, so $q^p \equiv q \bmod p^2$. However, one has $q^p = (1+2p)^p \equiv 1 \bmod p^2$ and $q = 1+2p \not\equiv 1 \bmod p^2$. This contradiction proves (a).

Finally, we prove (c). By (b), we have $p \neq 3$. By (d), we may assume that xyz is not divisible by 3. Considering the equation modulo 3, we find that $x \equiv y \equiv z \not\equiv 0 \bmod 3$. Then we have $\left(\frac{x+y\zeta}{3}\right) = \left(\frac{y+x\zeta}{3}\right)$, so from the lemma we obtain $\left(\frac{\zeta}{3}\right)^{-y/z} = \left(\frac{\zeta}{3}\right)^{-x/z}$. This implies that $\left(\frac{\zeta}{3}\right)^{y} = \left(\frac{\zeta}{3}\right)^{x}$, and by symmetry we have $\left(\frac{\zeta}{3}\right)^{x} = \left(\frac{\zeta}{3}\right)^{y} = \left(\frac{\zeta}{3}\right)^{z}$. From $3x^p \not\equiv 0 \bmod p$ we see that x, y, and z do not lie in a single residue class modulo p, and therefore we have $\left(\frac{\zeta}{3}\right) = 1$. As in the proof of (d), this implies (c).

1. J. W. S. Cassels, A. Fröhlich (eds), *Algebraic number theory, Proceedings of an Instructional Conference*, Academic Press, 1967.
2. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz*, Jber. Deutsch. Math.-Verein. Ergänzungsband **6** (1930), 1–204.