KUMMER'S PROOF OF FERMAT'S LAST THEOREM FOR REGULAR PRIMES: A MODERN VIEWPOINT

K. H. PARANJAPE

Introduction

Let us first recall a standard restatement:

Fermat's Last Theorem: There are no solutions to the following problem with (X, Y, Z) integers

$$\begin{aligned} X^p + Y^p + Z^p &= 0 \\ XYZ &\neq 0 \\ p \geq 3 & \quad \text{and a prime} \end{aligned}$$

The approach to the proof of Fermat's Last Theorem that is followed by A. Wiles in his recent attempt can be thought of as a particular case of the following tactic.

Suppose (X, Y, Z) is a counter-example to Fermat's Last Theorem.

(1) To such a counter-example we attach a representation

$$\rho_{(X,Y,Z)} : \mathrm{Gal}(\overline{\mathcal{Q}}/\mathcal{Q}) \to \mathrm{GL}_n(\mathcal{F}_p)$$

Moreover, we have *good* ramification properties for this representation. For example,
   (a) the representation is unramified outside p,
   (b) the representation has "good" ramification properties at p.

(2) The next step is to use our knowledge of Algebraic Number Theory to prove that such representations are impossible.

The proof of Kummer for the case of regular primes can also be reviewed in this light. First of all, Kummer's proof associates to every counter-example (X, Y, Z), a representation

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathcal{F}_p$$

where K is cyclotomic field of p-th roots of unity. Next, he gives a way of finding out which primes p are such that we have such a

representation. As he showed, there are indeed such primes and thus his proof works only for "regular" primes.

In section 1 we recall some computations in the cyclotomic field of p-th roots of unity. In section 2 we show how a counter-example to Fermat's Last Theorem (if it exists) can be used to construct a cyclic extension of order p of the cyclotomic field which is unramified *everywhere*. We review the Class number formula in section 3. Finally, in Section 4 we use this formula to check when such unramified extensions do indeed exist.

Most of the material in this note can be found in more detail (though in a more classical presentation) in the book of H. M. Edwards [1]. This re-examination of Kummer's proof was inspired by some remarks made by V. Kumar Murty during his lecture on the work of Wiles at the TIFR. I would like to thank A. Raghuram for his careful reading of the manuscript and numerous suggestions.

We fix a prime $p \geq 5$ throughout the discussion.

1. Arithmetic of prime cyclotomic fields

Let R denote the subring of complex numbers generated by $\omega = \exp(2\pi\iota/p)$; let K denote the quotient field of R, which is called the cyclotomic field of p-th roots of unity. We review some well-known facts about the ring R and the field K—mostly without proof.

The ring R is isomorphic to $\mathcal{Z}[X]/(\Phi_p(X))$, where

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1 = (X^p - 1)/(X - 1)$$

is an irreducible polynomial (a simple application of the Eisenstein criterion). The field K is a Galois extension of $\mathcal{Q}$ with Galois group $\mathcal{F}_p^*$; this is a cyclic group of order $(p-1)$. We use γ for a fixed choice of generator. We use $\overline{\alpha}$ to denote $\gamma^{(p-1)/2}(\alpha)$ since $\gamma^{(p-1)/2}$ is the restriction of complex conjugation to R.

The ring R is a Dedekind domain, i. e. unique factorization holds for ideals. The prime ideals in this ring are described as follows:

(1) If $q \in \mathcal{Z}$ is a prime number different from p. Then let f be the order of q in $\mathcal{F}_p^*$ and let $g = (p-1)/f$. Then there are g prime ideals $Q_1, \ldots, Q_g$ in R such that their norms are q^f.
(2) The element $\lambda = 1 - \omega$ is prime in R and $\lambda^{p-1} = (\text{unit}) \cdot p$.

A closed form expression for the generators of the group U of units of R is not known. However, the numbers

$$u_j = \gamma^j(\lambda)/\lambda = 1 + \omega + \cdots + \omega^{j-1}$$

are in R and are units there. The subgroup U_{cycl} of the group U of units of R generated by the u_j for $j = 2, \ldots, (p-1)$ is called the group of cyclotomic units. If u is a unit in R, then $\overline{u}/u$ is a root of unity in R. The roots of unity in R are all of the form $\pm\omega^j$ for some $j = 0, \ldots, p-1$. An element of R is a p-th power only if it is congruent to an integer modulo pR. It follows that $\overline{u}/u = \omega^j$ for some j (i. e. there is no minus sign).

Let L denote the subfield of K fixed by complex conjugation; let $S = L \cap R$. Then L is a Galois extension of $\mathcal{Q}$ with Galois group $\mathcal{F}_p^*/\{\pm 1\}$. No complex embeddings of K have image within real numbers while all complex embeddings of L have image within real numbers; in other words, K is purely imaginary and L is totally real. Again, S is a Dedekind domain and its ideals are described as follows:

(1) If $q \in \mathcal{Z}$ is a prime number different from p. Then let f' be the order of q in $\mathcal{F}_p^*/\{\pm 1\}$ and let $g' = (p-1)/2f'$. Then there are g' prime ideals $Q_1, \ldots, Q_g$ in R such that their norms are $q^{f'}$.
(2) The element $\mu = 1 - (\omega + \omega^{-1})$ is prime in R and $\mu^{(p-1)/2} = (\text{unit}) \cdot p$.

If u is a unit in R, then we have seen that $\overline{u}/u = \omega^r$ for some integer r. But then $r \equiv 2s \pmod{p}$ for some integer s; hence $u_1 = \omega^{-s}u$ is in S. Hence, any unit in R is the product of a root of unity and a unit in S.

If I is any ideal in S then IR is principal in R if and only if I is principal in S. Hence the homomorphism from the class group of S to that of R is injective. In particular the order h of the class group of R is divisible by the order h_+ of the class group of S.

If we have a unit u in R such that it is congruent to an integer modulo pR and if u is itself *not* a p-th power, then the field extension of K obtained by adjoining a p-th root of u is a cyclic extension of K of order p which is unramified everywhere.

Finally we have a fact from Class Field theory. If there is an ideal I in R such that I^p is principal and I is not principal, then there is a cyclic entension of K of order p which is unramified everywhere. This follows from the identification of the class group of R with the Galois group of the maximal unramfied abelian extension of K. Now we use the fact that if an abelian group has an element of order p, then it has a non-trivial character of order p.

2. Construction of cyclic cover

The aim is to show that if we have a counter-example to Fermat's Last Theorem, then there is a cyclic extension of order p of K which is unramified everywhere. As is usual we can assume that the given

counter-example (X, Y, Z) has the property that these are mutually co-prime integers.

Case 1: $p \not| XYZ$**.** First of all we see easily that (X, Y, Z) are not all congruent modulo p. If not, we have

$$3X \equiv X + Y + Z \equiv X^p + Y^p + Z^p \equiv 0 \pmod{p}$$

Now, we are assuming that $p \geq 5$ and so we obtain $X \equiv 0 \pmod{p}$; this contradicts our hypothesis for Case 1.

Secondly, we see that $(X+\omega^j Y)$ are mutually co-prime in R as j runs over $0, \ldots, p-1$. If not, then we have a prime ideal P in R containing $(X + \omega^j Y, X + \omega^k Y)$. Then this ideal P contains $(1 - \omega^{j-k})Y$. Now from the factorisation

$$(-Z)^p = X^p + Y^p = (X + Y)(X + \omega Y) \cdots (X + \omega^{p-1} Y)$$

we see that P contains Z. Hence, by the assumption that (X, Y, Z) are mutually co-prime we see that P contains $(1-\omega^l)$ for some $0 \leq l \leq p-1$. By the description of prime ideals in R as in section 1 we see that $P = \lambda R$. But then Z is a multiple of p which contradicts our hypothesis in Case 1.

By the above paragraph and unique factorization of ideals we see that we have ideals I_j of R such that $I_j^p = (X + \omega^j Y)R$. Assume I_1 is principal; then we have an equation

$$(X + \omega Y) = u \cdot \alpha^p$$

for some $\alpha \in R$ and u a unit in R. Applying complex conjugation we obtain

$$(X + \omega^{-1} Y) = \overline{u} \cdot \overline{\alpha}^p$$

By the results mentioned in section 1 we have $\omega^r \overline{u} = u$ for some r. Moreover, α^p is congruent to an integer modulo pR and hence is congruent to its own complex conjugate. Thus we obtain an equation

$$X + \omega Y - \omega^r X - \omega^{r-1} Y \equiv 0 \pmod{p}$$

Now it follows from the description of R given in Section 1 that it is a free abelian group with basis consisting of any $(p-1)$ elements of the set $\{1, \omega, \ldots, \omega^{p-1}\}$. From this and the fact that X and Y are prime to p it follows that $r = 1$ and $X \equiv Y \pmod{p}$.

By similar reasoning interchanging the roles of Y and Z we can conclude that there is an ideal J_1 such that $J_1^p = (X + \omega Z)$. Assuming J_1 is principal we see by an argument like the one above that $X \equiv Z \pmod{p}$. But as seen above the two congruences

$$X \equiv Y \pmod{p} \text{ and } X \equiv Z \pmod{p}$$

contradict the hypothesis of Case 1. Hence, either I_1 or J_1 must be non-principal. But then by the principal result of Class Field theory as mentioned in section 1 we have required cyclic extension of K.

Case 2: $p|XYZ$**.** We may assume that $Z = p^k Z_0$ and (p, X, Y, Z_0) are mutually co-prime. By writing $p = (\text{unit}) \cdot \lambda^{(p-1)}$ in the ring R, we obtain an equation of the form

$$U^p + V^p + (\text{unit})\lambda^{mp} W^p = 0 \text{ with } m > 0$$

where (U, V, W) are in R so that (U, V, W, λ) are mutually co-prime. Let (U, V, W) be a collection of elements of R that satisfy such an equation with m the least possible. Then λ divides one of the factors $(U + \omega^j V)$. But then we have

$$(U + \omega^j V) - (U + \omega^k V) = \omega^j (1 - \omega^{k-j}) V = (\text{unit}) \cdot \lambda V$$

and thus, λ divides all the factors $(U + \omega^j V)$. Moreover, since V is co-prime to p and thus λ as well, we see that $(U + \omega^j V)/\lambda$ have distinct residue classes modulo λR. But then, by the pigeon-hole principle there is at least one $0 \leq j \leq (p-1)$ such that $(U + \omega^j V)$ is divisible by λ^2 in R. Replacing V by $\omega^j V$ we may assume that $(U + V)$ is divisible by λ^l for some $l > 1$. Hence we may write

$$\begin{aligned} U + V &= \lambda^l a_0 \\ U + \omega^k V &= \lambda a_k; \text{ for } k > 0 \end{aligned}$$

where all the a_k are elements of R that are co-prime to λ and with each other (as in the previous case). This gives us the identity $l + (p-1) = mp$ or equivalently $l = (m-1)p + 1$. Since $l \geq 2$ we have $m \geq 2$.

Now by unique factorisation of ideals in R we see that there are ideals I_j in R such that $I_j^p = a_j R$. Assume that I_0, I_1 and I_{p-1} are principal, then we have the equations

$$\begin{aligned} U + V &= \lambda^l \cdot u \cdot b_0^p \\ U + \omega V &= \lambda \cdot v \cdot b_1^p \\ U + \omega^{-1} V &= \lambda \cdot w \cdot b_{-1}^p \end{aligned}$$

for some units u, v and w in R and some elements b_0, b_1 and b_{-1} in R. Eliminating U and V from these equations we obtain

$$\lambda^l \cdot u \cdot b_0^p - \lambda \cdot v \cdot b_1^p = \omega(\lambda \cdot w \cdot b_{-1}^p - \lambda^l \cdot u \cdot b_0^p)$$

which becomes

$$b_1^p + v_1 \cdot b_{-1}^p + \lambda^{l-1} \cdot v_2 b_0^p = 0$$

where v_1 and v_2 are units (we use here the fact that $1 + \omega$ is a unit in R). Modulo pR the last term on the left-hand side vanishes since $l \geq p > (p-1)$. Thus we see that v_1 is congruent to a p-th power

and thus an integer modulo pR. By section 1 we have a representation of Galois as required, unless v_1 is a p-th power. If $v_1 = v_3^p$, then $(U, V, W) = (b_1, v_3 b_{-1}, b_0)$ satisfy

$$U^p + V^p + (\text{unit})\lambda^{(m-1)p} W^p = 0$$

which contradicts the minimality of m since we have seen that $m \geq 2$. Thus, either we have constructed a cyclic extension of the required type or one of I_0, I_1, I_{p-1} is non-principal. But then again by the principal result of Class Field theory we have a cyclic extension as required.

3. Transcendental computation of the Class number

We first need to introduce the Dedekind zeta function for a number field K, and its Euler product expansion

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s} = \prod_Q \frac{1}{(1 - \frac{1}{N(Q)^s})}$$

where the sum runs over all ideals I of R and the product runs over all prime ideals Q of R. The two expressions give us two ways of computing $\lim_{s\to 1}(s-1)\zeta_K(s)$. The left-hand side is expressed in terms of "arithmetic" invariants and the right-hand side in terms of invariants for the Galois group. The resulting identity gives a way for computing the Class number h of K.

The left-hand limit can be computed to be

$$\lim_{s\to 1}(s-1)\sum_I \frac{1}{N(I)^s} = \lim_{r\to\infty} \frac{\#\{I \mid N(I) \leq r\}}{r}$$

The set $\{I \mid N(I) \leq r\}$ can be split according to ideal classes. We try to compute for each ideal class C,

$$z(C) = \lim_{r\to\infty} \frac{\#\{I \in C \mid N(I) \leq r\}}{r}.$$

Fixing an ideal $I_0 \in C$, this latter set is bijective to the set $\{aR \subset I_0^{-1} \mid N(a) \leq r \cdot N(I_0)^{-1}\}$. (Here $N(a)$ denotes the modulus of the norm of a.)

We have a natural embedding $K \hookrightarrow K \otimes_{\mathcal{Q}} \mathcal{R}$. The image of $J = I_0^{-1}$ is a lattice in $K \otimes_{\mathcal{Q}} \mathcal{R}$. Let Λ denote the image of $J - \{0\}$ in the quotient $\mathcal{S} = (K \otimes_{\mathcal{Q}} \mathcal{R})^*/U$ where U is the image of the group of units in R under the above embedding. There is a natural homomorphism $N : \mathcal{S} \to \mathcal{R}^*$ which restricts to the modulus of the norm on the image of K. We obtain a natural bijection between $\{aR \subset I_0^{-1} \mid N(a) \leq r\}$ and $\{l \in \Lambda \mid N(l) \leq r\}$. Let Λ_r denote the image of $(1/r)J - \{0\}$ in

$\mathcal{S}$, then we have a natural bijection between $\{l \in \Lambda \mid N(l) \leq r^d\}$ and $\{l \in \Lambda_r \mid N(l) \leq 1\}$, where d denotes the degree of K oover $\mathcal{Q}$.

Let $\mathcal{S}_{\leq 1}$ denote locus of $l \in \mathcal{S}$ such that $N(l) \leq 1$. Let μ denote the Haar measure on $K \otimes_{\mathcal{Q}} \mathcal{R}$. This is invariant under the action of U and thus gives a measure also denoted by μ on $\mathcal{S}$. Since J is a lattice in $K \otimes_{\mathcal{Q}} \mathcal{R}$ we have

$$\lim_{r\to\infty} \frac{\#\{l \in \Lambda_r \mid N(l) \leq 1\}}{r^d} = \frac{\mu(\mathcal{S}_{\leq 1})}{\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/J)}$$

Moreover, the denominator can be re-written

$$\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/J) = N(J)\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/R).$$

In particular, we see that the limit $z(C)$ is independent of the class C. Let $(K \otimes_{\mathcal{Q}} \mathcal{R})_1^*$ denote the kernel of the norm map. This is a group and thus we have a Haar measure ν on it. One shows that

$$\mu(\mathcal{S}_{\leq 1}) = \nu((K \otimes_{\mathcal{Q}} \mathcal{R})_1^*/U)$$

Combining the above calculations one obtains

$$\lim_{s\to 1}(s-1) \cdot \zeta_K(s) = h \cdot \frac{\nu((K \otimes_{\mathcal{Q}} \mathcal{R})_1^*/U)}{\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/R)}$$

This often called the "Class number formula" for K. Note that the denominator can be computed in closed form in terms of the discriminant D of the field K and the number of pairs of conjugate complex embeddings r_2 of K.

$$\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/R) = \frac{1}{2^{r_2}} \cdot \sqrt{|D|}$$

However, the numerator is in general more complicated since it involves computing the group of units of K.

To expand the right-hand term we restrict our attention to abelian extensions K of $\mathcal{Q}$. The product term on the left can be first grouped according to rational primes

$$\prod_{Q} \frac{1}{(1 - \frac{1}{N(Q)^s})} = \prod_{q} \prod_{Q|q} \frac{1}{(1 - \frac{1}{N(Q)^s})}$$

Now for each rational prime q which is unramified in K we have

$$\prod_{Q|q} \frac{1}{(1 - \frac{1}{N(Q)^s})} = \prod_{\chi} \frac{1}{(1 - \frac{\chi(q)}{q^s})}$$

where χ runs over all characters of the Galois group and $\chi(q) = \chi(\mathrm{Frob}_q)$ is the value of χ on a Frobenius element associated with q.

We define the Dirichlet L-series and their Euler product formulas as follows

$$L(s,\chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{(1-\frac{\chi(p)}{p^s})}$$

where we set $\chi(p) = 0$ when χ is ramified at p. We also define the additional factor

$$F(s) = \prod_{p \text{ ramified}} \frac{1}{(1-\frac{1}{p^{f_p}})^{g_p}}$$

where the product runs over all ramified primes and f_p denotes the residue field extension over p and g_p the number of distinct primes in K lying over p. The product expansion of $\zeta_K(s)$ becomes

$$\zeta_K(s) = F(s) \cdot \prod_\chi L(s,\chi).$$

Thus the computation of the limit can be reduced to the corresponding computation for the Dirichlet L-series. For the case of the unit character we get by comparison with the zeta function

$$\lim_{s\to 1}(s-1)F(s)L(s,1) = 1.$$

So the right-hand limit gives

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \prod_{\chi\neq 1} L(1,\chi).$$

There is a positive integer m such that χ is determined on classes modulo m and χ is zero on all primes p dividing it; m is called the *conductor* of χ. We rewrite the L-function associated with χ as follows

$$L(s,\chi) = \sum_{x\in(\mathcal{Z}/m\mathcal{Z})^*} \left(\chi(x) \cdot \sum_{n\equiv x \pmod m} \frac{1}{n^s} \right)$$

The latter sum can be rewritten using the identity

$$\sum_{i=0}^{m-1} \omega^{xi} = \begin{cases} 0, \text{ if } x \not\equiv 0 \pmod m \\ m, \text{ if } x \equiv 0 \pmod m \end{cases}$$

where ω is a primitive m-th root of unity. The second sum then becomes

$$\sum_{n\equiv x \pmod m} \frac{1}{n^s} = \frac{1}{m} \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{i=0}^{m-1} \omega^{(x-n)i}$$

Thus we obtain

$$L(s,\chi) = \frac{1}{m}\sum_{i=0}^{m-1}\left(\sum_{x\in(\mathcal{Z}/m\mathcal{Z})^*}\chi(x)\omega^{ix}\right)\cdot\sum_{n=1}^{\infty}\frac{\omega^{-in}}{n^s}$$

The expression

$$\tau_i(\chi) = \sum_{x\in(\mathcal{Z}/m\mathcal{Z})^*}\chi(x)\omega^{ix}$$

is called the Gaussian sum associated with the integer i and the character χ. If χ is not the unit character then $\tau_0(\chi) = 0$. Moreover, if $i \neq 0$ then we have the identity

$$\sum_{n=1}^{\infty}\frac{\omega^{-in}}{n} = -\log(1-\omega^{-i})$$

Hence, we obtain the formula when χ is not the unit character

$$L(1,\chi) = -\frac{1}{m}\sum_{i=1}^{m-1}\tau_i(\chi)\cdot\log(1-\omega^{-i})$$

4. Divisiblity of the Class number by p

Combining the results of sections 1 and 2 we have shown that any counter-example to Fermat's Last theorem for a prime $p \geq 5$ leads to a non-trivial representation

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathcal{F}_p$$

which is unramified everywhere; here K denotes the subfield of complex numbers generated by the p-th roots of unity. Kummer called primes which admit such representations *irregular*. He showed that there are indeed such primes ($p = 37$ is one such) and hence this particular attempt to prove Fermat's Last theorem fails. We now wish to show how one goes about checking whether a prime is *irregular*.

We apply the results of Section 3 in the special case where K is the prime cyclotomic field of section 1 and also to the totally real subfield L.

First of all we use the divisibility of the class number h of R by the class number h_+ of S to write $h = h_+ \cdot h_-$ for some integer h_-. Let W denote the (finite cyclic) group of roots of unity in K. Then we have $U = W \cdot U_+$, where U_+ denotes the group of units in S and so $\#(U/U_+) = \#(W/\{\pm 1\}) = p$. We have the natural inclusion $L \otimes_{\mathcal{Q}} \mathcal{R} \hookrightarrow K \otimes_{\mathcal{Q}} \mathcal{R}$ from which we obtain the isomorphism

$$(K \otimes_{\mathcal{Q}} \mathcal{R})_1^*/(L \otimes_{\mathcal{Q}} \mathcal{R})_1^* = (\mathcal{C}_1^*/\mathcal{R}_1^*)^{(p-1)/2}$$

since $(p-1)/2$ is the degree of L over $\mathcal{Q}$. From this we deduce that

$$\nu((K \otimes_{\mathcal{Q}} \mathcal{R})_1^*/U) = \frac{1}{p} \cdot \nu(\mathcal{C}_1^*/\mathcal{R}_1^*)^{(p-1)/2} \cdot \nu((L \otimes_{\mathcal{Q}} \mathcal{R})_1^*/U_+)$$

The formula for computing discriminants yields

$$\mu(K \otimes_{\mathcal{Q}} \mathcal{R}/R) = \mu(L \otimes_{\mathcal{Q}} \mathcal{R}/S)^2 \cdot p^{1/2}$$

since p is the norm of the relative discrimant. Thus the class number formulas for K and L then give a formula for h_-

$$\frac{h_- \cdot \nu(\mathcal{C}_1^*/\mathcal{R}_1^*)^{(p-1)/2}}{p^{3/2} \cdot \mu(L \otimes_{\mathcal{Q}} \mathcal{R}/S)} = \prod_{\chi(-1)=-1} L(1,\chi)$$

Hence h_- can be computed explicitly and in closed form. In particular, the divisibility of h_- by p is an easily computable criterion.

The divisibility of h_+ by p is more complicated. As remarked earlier, the term $\nu((L\otimes_{\mathcal{Q}}\mathcal{R})_1^*/U_+)$ is difficult to compute. However, we have the subgroup $U_{+,\mathrm{cycl}} = U_+ \cap U_{\mathrm{cycl}}$ and one can compute $\nu((L\otimes_{\mathcal{Q}}\mathcal{R})_1^*/U_{+,\mathrm{cycl}})$. In fact one shows that

$$\nu((L \otimes_{\mathcal{Q}} \mathcal{R})_1^*/U_{+,\mathrm{cycl}}) = \mu(L \otimes_{\mathcal{Q}} \mathcal{R}/S) \cdot \prod_{\chi \text{ even}} L(1,\chi)$$

where the product runs over all non-trivial characters χ such that $\chi(-1) = 1$. The class number formula for h_+ becomes

$$h_+ = [U_+ : U_{+,\mathrm{cycl}}] = [U : U_{\mathrm{cycl}}].$$

This is the first coincidence that makes Kummer's calculations possible.

From the above identity we see that if p divides h_+ then we have a real unit u such that its p-th power is a cyclotomic unit but u is not itself cyclotomic. Hence $v = u^p$ is a cyclotomic unit which is congruent to an integer modulo pS. If we find a $w \in U_{\mathrm{cycl}}$ such that $v = w^p$ then one shows easily that u is itself a cyclotomic unit. Let Q denote the quotient group $(S/pS)^*/(\mathcal{Z}/p\mathcal{Z})^*$. We obtain a natural homomorphism

$$m : U_{\mathrm{cycl}} \otimes (\mathcal{Z}/p\mathcal{Z}) \to Q$$

which is represented by a square matrix with entries from $\mathcal{F}_p$. The preceding remarks imply that $p|h_+$ only if $\det(m) = 0$. The second coincidence that makes Kummer's calculation work is that $\det(m) \equiv h_- \pmod{p}$.

Thus we see that $p|h$ if and only if $p|h_-$. Hence we can easily check which primes are regular.

References

[1] H. M. Edwards, *Fermat's last theorem*, Graduate Texts in Mathematics, vol. 50, Springer-Verlag, New York Berlin Heidelberg, 1977.

School of Mathematics, TIFR, Homi Bhabha Road, Bombay 400 005, India