11 Remarks on Fermat's Last Theorem and an approach of Gauss

Recall the Fermat equation $x^n + y^n = z^n$. For $n = 2$, this leads to Pythogorean triples and we classified all the solutions in this case.

Theorem (A. Wiles) ('97): For $n \geq 3$, $x^n + y^n = z^n$ has no positive integral solutions.

There is no way we can prove this magnificient result in this class.

Note: To prove this, it suffices to prove in the cases where $n = 4$ and when $n = p$, where p is any odd prime.

Reason: If $m|n$, then any solution of $u^n + v^n = w^n$ will give a solution for m, namely $(u^{n/m})^m + (v^{n/m})^m = (w^{n/m})^m$.

Moreover, for any $n \geq 3$, n will be divisible by 4 or by an odd prime p.

We also proved in the first week that $x^4 + y^4 = z^4$ has no integral solutions for. (In fact, we showed Fermat's result that $x^4 + y^4 = w^2$ has no integral solutions.) Consequently, the key fact needed to be proven is that $x^p + y^p = z^p$ has no solution for any odd prime.

This gets split into two cases:

$$\begin{aligned} \text{Case I:} &\quad p \nmid xy\,z. \\ \text{Case II:} &\quad p \mid xy\,z. \end{aligned}$$

Proposition (Gauss). Suppose the congruence

$$(*) \qquad x^p + y^p \equiv (x+y)^p \pmod{p^2}$$

has no *non-trivial* solutions, i.e. with none of x, y, $x + y \equiv 0 \pmod{p}$. Then Case I of FLT holds for p, i.e.

$$\nexists\, x, y, z \in \mathbb{Z}_{>0}, \quad p \nmid x\,y\,z, \text{ such that } x^p + y^p = z^p.$$

Note:

$$(x+y)^p = \sum_{j=p}^{p} \binom{p}{j} x^j y^{p-j}, \qquad \binom{p}{j} = \frac{p!}{(p-j)!j!}$$

If $j \neq 0$ or p, then $\binom{p}{j}$ is divisible by p. Since $(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}$, we get

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Proof of Prop.

Suppose we have positive integers x, y, z, with $p \nmid xyz$, such that $x^p + y^p = z^p$. We have just seen that $x^p + y^p \equiv (x+y)^p \pmod{p}$, so $z^p \equiv (x+y)^p \pmod{p}$.

Moreover, we have the Little Fermat Theorem, which says that $x^p \equiv x \pmod{p}$, $z^p \equiv z \pmod{p}$, $y^p \equiv y \pmod{p}$, and $(x+y)^p \equiv x + y \pmod{p}$. Consequently, $z \equiv x + y \pmod{p}$, i.e. $z = x + y + mp$, for some $m \in \mathbb{Z}$.

Since $x^p + y^p = z^p$, we get

$$\begin{aligned} x^p + y^p = (x+y+mp)^p &= \sum_{i=0}^{p} \binom{p}{i} (x+y)^i (mp)^{p-i} \\ &= (mp)^p + p(x+y)(mp)^{p-1} + \cdots + p(x+y)^{p-1}(mp) + (x+y)^p. \end{aligned}$$

Therefore $x^p + y^p \equiv (x+y)^p \pmod{p^2}$

Difficulty:

If $p \equiv 1 \pmod{3}$, one can always solve the congruence $x^p + y^p \equiv (x+y)^p \pmod{p^2}$. So Gauss's Proposition doesn't help us. On the other hand, when $p \equiv 2 (\mathrm{mod}\, 3)$, for many small primes, $x^p + y^p \equiv (x+y)^p \pmod{p^2}$ has no solution.

Still, there are primes $p \equiv 2 \pmod{3}$ for which $\exists$ solutions to this congruence. This happens for 13 primes less than 1000. For example, when $p = 59$, $1^{59} + 3^{59} \equiv 4^{59} \pmod{59^2}$.