Number Theory Section Summary: 11.2
Fermat's Last Theorem

1. Summary

So we left things at all solutions of

$$x^2 + y^2 = z^2 \tag{1}$$

which can be written as

$$(2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2$$

for integers $s > t > 0$ such that $\gcd(s,t) = 1$ with $s \not\equiv t \pmod 2$. In particular, there ARE integer solutions of that equation (1); so what about

$$x^n + y^n = z^n?$$

One observation is that, if $n = pq$, then

$$(x^p)^q + (y^p)^q = (z^p)^q$$

and

$$(x^q)^p + (y^q)^p = (z^q)^p$$

so that we simultaneously have solutions for all powers which are factors of n. Thus it suffices to ask if we can solve

$$x^p + y^p = z^p$$

for primes p: if we can't solve it for the prime factors of n, then we can't solve it for n itself.

Since we CAN find solutions for $p = 2$, it's certainly possible that we have solutions for $n = 2^k$, for $k \geq 2$. Fermat, however, took care of that....

Andrew Wiles recently (1994) proved that no solutions in integers exist for any power n greater than 2. In this section, we see how Fermat (who professed to have a proof of this theorem) solved the case of $n = 4$.

2. Theorems

Theorem 11.3: The Diophantine equation $x^4+y^4 = z^2$ has no solution in the positive integers x, y, and z.

Proof: by Fermat's method of "infinite descent": one obtains from a triple a strictly smaller triple, and so on *ad infinitum*; but the positive integers cannot be reduced *ad infinitum* – contradiction!

Corollary: The equation $x^4 + y^4 = z^4$ has no solution in the positive integers x, y, and z.

Corollary: The equation $x^{4k}+y^{4k} = z^{4k}$ has no solution in the positive integers x, y, and z.

Hence, the only exponents of interest left to prove are odd primes....

Theorem 11.4: The Diophantine equation $x^4-y^4 = z^2$ has no solution in the positive integers x, y, and z.

3. Properties/Tricks/Hints/Etc.

- Fermat (1637) writes

  "It is impossible to write a cube as a sum of two cubes, a fourth power as the sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have discovered a truly wonderful proof, but the margin is too small to contain it."

  Fermat proved the case $n = 4$, and hence $n = 4k$.
- Euler (1770) proved the result for the case $p = 3$;
- Dirichlet and Legendre (1825) independently proved the case $p = 5$;
- Lamé (1829) proved the case $p = 7$;

- Kummer (mid 1800s) proved the result for a large **class** of primes p (called the *regular primes*);
- Faltings (1983) proved that all powers $n > 2$ could have only finitely many triples as solutions; and
- Andrew Wiles (1994) proved the whole enchilada....

Proof of 11.3: (by contradiction)

$x^4 + y^4 = z^2$ has no soln. in the positive integers.

Assume that $\exists$ a soln. in pos. integers (x, y, z). Choose a soln. with the minimal value of z (there must be one by well-ordering).

Claim: $\gcd(x, y) = 1$. Assume not: $\gcd(x, y) = d > 1$. Then $d \mid z \Rightarrow$ we could have factored out a term involving d:

$$(dx_1)^4 + (dy_1)^4 = d^4(x_1^4 + y_1^4) = z^2 \Rightarrow$$

$d^2 \mid z$: $z = d^2 z_1 \Rightarrow$

$$x_1^4 + y_1^4 = z_1^2 ;$$

but $z_1 < z$, which contradicts the choice of z as minimal. So $\gcd(x, y) = 1$.

Rewrite $x^4 + y^4 = z^2$ as

$$(x^2)^2 + (y^2)^2 = z^2 ,$$

i.e. (x^2, y^2, z) is a Pythagorean triple - is it primitive? Is $\gcd(x^2, y^2, z) = 1$?

$$\gcd(x,y) = 1 \Rightarrow \gcd(x^2, y^2) = 1 \Rightarrow$$

$$\gcd(x^2, y^2, z) = 1.$$

So this triple is primitive, & we can do the "s-t" thing:

$$\left.\begin{aligned} x^2 &= 2st \\ y^2 &= s^2 - t^2 \\ z &= s^2 + t^2 \end{aligned}\right\} \text{ where } \begin{cases} s > t > 0 \\ s \not\equiv t \pmod 2 \\ \gcd(s,t) = 1 \end{cases}$$

Which of s & t is even? Well, y is odd, so y^2 is odd: $y \equiv 1$ or $3 \pmod 4 \Rightarrow y^2 \equiv 1 \pmod 4$

Assume s is even:

$$\begin{aligned} y^2 = s^2 - t^2 &\equiv 0 - 1 \pmod 4 \\ &\equiv -1 \pmod 4 \end{aligned}$$

Contradiction. Hence t is even:

$$\therefore \quad t = 2r \quad \exists r.$$

Now $$x^2 = 2st = 2 \cdot s \cdot 2r = 4sr$$

$$\therefore \left(\frac{x}{2}\right)^2 = sr$$

If $\gcd(s,r) = 1$, then we can invoke lemma 2 from §11.1. $\gcd(s,t) = \gcd(s, 2r) = 1 \Rightarrow$ $\gcd(s,r) = 1$. So we can invoke lemma 2:

$\therefore \quad s = z_1^2$

$r = w^2$

Back to $y^2 = s^2 - t^2$, or

$$t^2 + y^2 = s^2$$

(which is primitive since $\gcd(t,s) = 1$). So let's use the "s-t" trick <u>again</u>:

$$t = 2uv = 2r$$

$$\therefore \quad uv = r = w^2$$

u & v are relatively prime, so that u & v are squares by lemma 2:

$$u = x_1^2$$

$$v = y_1^2$$

$$\therefore \quad s = u^2 + v^2 = x_1^4 + y_1^4 = z_1^2,$$

so (x_1, y_1, z_1) also solve the original equation; the problem is that

$$z_1 \leq z_1^2 = s < s^2 < s^2 + t^2 = z$$

contradicting the choice of z as minimal.

$\therefore$ $\nexists$ solns of $x^4 + y^4 = z^2$

in the positive integers.

Suppose $\exists$ a soln. in the pos. integers to

$$x^4 + y^4 = z^4 = (z^2)^2 ;$$

then we have a soln to

$$x^4 + y^4 = w^2$$

#4 p247

a. $x^2 + y^2 = z^2 - 1$

$x^2 - y^2 = w^2 - 1$

$x = 2n^2$ & $y = 2n$ $\quad n \geq 1$

$$\boxed{\begin{aligned} z &= 2n^2 + 1 \\ w &= 2n^2 - 1 \end{aligned}}$$

c. $x^2 + y^2 = z^2 + 1$

$x^2 - y^2 = w^2 + 1$

has infinitely many Solns. $x, y, z,$ & w.

$z = 4n^2(2n^2 + 1)$

$w = 4n^2(2n^2 - 1)$

b. $x^2 + y^2 = z^2$

$x^2 - y^2 = w^2$

has no pos integer solns

$2x^2 = z^2 + w^2$ ...

$$(x^2+y^2)(x^2-y^2) = x^4 - y^4 = z^2w^2$$
$$= (zw)^2$$

which has no solns in the pos. integers.