Number Theory Section Summary: 11.2

Fermat's Last Theorem

1. Summary

So we left things at all solutions of

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

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. $\Rightarrow \quad x^4+y^4=(z^2)^2$ $\qquad x^8+y^8=z^8$

Corollary: The equation $x^{4k}+y^{4k}=z^{4k}$ has no solution in the positive integers x, y, and z. $\qquad (x^2)^4+(y^2)^4=(z^2)^4$

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....

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

Proof (by contradiction) : ① Assume that there is a solution triple, (x, y, z). By well-ordering there has to be one (or possibly several) with a smallest value of z. Assume (x, y, z) is a solution with minimal z.

② $\gcd(x, y) = 1$: otherwise $\gcd(x, y) = d \neq 1$, so

$x = dx_1$

$y = dy_1$

and $(dx_1)^4 + (dy_1)^4 = z^2 \Rightarrow d^4 \mid z^2 \Rightarrow$

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

hence $x_1^4 + y_1^4 = z_1^2$ with $z_1 < z$,

contradicting minimal z. So $\gcd(x, y) = 1$.

③ Rewrite $x^4 + y^4 = z^2$ as

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

So (x^2, y^2, z) is a Pythagorean triple. Is it primitive? Yes, since $\gcd(x^2, y^2) = 1$. So let's use Theorem 11.1:

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

(4) Let's establish which of s & t is even:

Assume s is even. Now y was odd, so

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

Contradiction. Hence t is even; call it

$$t = 2r.$$

(5) Plug this value of t into $x^2 = 2st$:

$$x^2 = 4sr$$

or

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

(Lemma 2 asserts that if s & r are rel. prime, then they're both squares.)

$\gcd(s,t) = 1$: $\exists\, a, b$ integers such that

$$as + bt = 1, \text{ or}$$

$$as + (b\,2)r = 1 \implies \gcd(s,r) = 1$$

Hence we can write

$$s = z_1^2$$
$$r = w^2$$

⑥ Now we'll go back to $y^2 = s^2 - t^2$, or

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

(a primitive triple since $\gcd(s,t)=1$). Let's use Theorem 11.1 again:

$$\left.\begin{aligned} t &= 2uv \\ y &= u^2 - v^2 \\ s &= u^2 + v^2 \end{aligned}\right\} \quad \begin{aligned} &\gcd(u,v) = 1 \\ &u \not\equiv v \pmod 2 \end{aligned}$$

⑦ Now we'll reuse Lemma 2: since

$$t = 2r = 2uv \quad \text{so}$$

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

$$\begin{aligned} u &= x_1^2 \\ v &= y_1^2 \end{aligned} \qquad (\text{by lemma 2, with } \gcd(u,v)=1)$$

⑧ Exciting conclusion:

$$s = u^2 + v^2 = z_1^2$$

$$(x_1^2)^2 + (y_1^2)^2 = z_1^2$$

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

except that

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

+ z was chosen to be minimal.

Contradiction.

Therefore there are no solutions to the equation $x^4 + y^4 = z^2$ in positive ints.

#4 p 247

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

has infinitely many solns in positive integers x, y, w, z

Consider $x = 2n^2$ & $y = 2n$ for $n \geq 1$

$$\left.\begin{array}{l}(2n^2)^2 + (2n)^2 = z^2 - 1 \\ (2n^2)^2 - (2n)^2 = w^2 - 1\end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{l}4n^4 + 4n^2 = z^2 - 1 \\ 4n^4 - 4n^2 = w^2 - 1\end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{l}4n^4 + 4n^2 + 1 = z^2 \\ 4n^4 - 4n^2 + 1 = w^2\end{array}\right\} \Rightarrow \begin{array}{l}(2n^2+1)^2 = z^2 \\ (2n^2-1)^2 = w^2\end{array}$$

So $z = 2n^2 + 1 > 0$
$w = 2n^2 - 1 > 0$

& each value of n produces a solution, $n \geq 1$.

(c)

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

has infinitely many solutions x, y, w, z.

Let

$x = 8n^4 + 1$

$y = 8n^3$

$n \geq 1$

$$(8n^4+1)^2 + (8n^3)^2 = z^2 + 1$$
$$(8n^4+1)^2 - (8n^3)^2 = w^2 + 1$$

$$64n^8 + 16n^4 \cancel{+1} + 64n^6 = z^2 \cancel{+1}$$

$$64n^8 + 16n^4 \cancel{+1} - 64n^6 = w^2 \cancel{+1}$$

$$16n^4\left(4n^4 + 4n^2 + 1\right) = z^2$$

$$16n^4\left(4n^4 - 4n^2 + 1\right) = w^2$$

$$16n^4\left(2n^2 + 1\right)^2 = z^2$$

$$16n^4\left(2n^2 - 1\right)^2 = w^2$$