# MATH 115, SUMMER 2012 <br> LECTURE 25 

JAMES MCIVOR

## 1. Fermat's Last Theorem, $n=4$ Case

Recall that one of the most famous problems in number theory (indeed, in all of mathematics!) was Fermat's Last Theorem. The question was whether, for a give value of $n$, there existed positive integers $x, y, z$ satisfying the equation

$$
x^{n}+y^{n}=z^{n}
$$

Fermat scribbled somewhere that he had a proof that there were NO solutions when $n>2$, but nobody ever found his proof, and it took until the 1990s for mathematicians to prove it!

Today we prove it in the special case $n=4$. Surprisingly, this, and not $n=3$, is the easiest case.

First observe that it follows from the following result:
Theorem 1. The equation

$$
x^{4}+y^{4}=z^{2}
$$

has no solution in positive integers.
For if we had a solution to the Fermat equation $x^{4}+y^{4}=z^{4}$, then replacing $z$ by $z^{2}$ would give a solution to the equation in the theorem.

## 2. Fermat's "Method of Descent"

This is a brilliant idea: we show that there can be no solution, for if there were, we could always produce another solution with a smaller value of $z$ - this is the "descent". This is a contradiction, because, e.g., we might get to $z=1$, and there is no smaller positive integer.

How do we establish the descent ${ }^{1}$ ?

- Suppose we have a solution $x, y, z$ to $x^{4}+y^{4}=z^{2}$.
- Then $x^{2}, y^{2}, z$ is a Pythagorean triple.
- we can assume it's primitive, for if some prime $p$ divides all three, then $p \mid x$ and $p \mid y$, so we can divide out the $p$ and get a new triple $\left(\frac{x}{p}\right)^{2},\left(\frac{y}{p}\right)^{2}, \frac{z}{p}$. Continue doing so until they're relatively prime.
- By the results of the last lecture, we can assume $x$ is even and $y$ is odd.
- Also from last lecture, we know there are coprime integers $a, b$ such that

$$
\begin{aligned}
x^{2} & =a^{2}-b^{2} \\
y^{2} & =2 a b \\
z & =a^{2}+b^{2}
\end{aligned}
$$

[^0]- Look at $y^{2}=2 a b$. Since $2 a b$ is a square, and $a, b$ are coprime, one of $a, b$ must be two times an odd square, and the other must be an odd square.
- Now look at the first equation: it says $x^{2}+b^{2}=a^{2}$, and since $a, b$ are coprime, $x, y, z$ form a primitive Pythagorean triple.
- Thus we can find relatively prime $r, s$ such that

$$
\begin{aligned}
x & =r^{2}-s^{2} \\
a & =2 r s \\
b & =r^{2}+s^{2}
\end{aligned}
$$

- we said above that one of $a, b$ was 2 times an odd square, and the other an odd square; now we know that $a$ is even. So $a=2 m^{2}$ and $b=n^{2}$, where $m, n$ are odd.
- now we have

$$
2 m^{2}=a=2 r s, \quad \text { so } \quad m^{2}=r s
$$

-by a lemma from last lecture, since $r, s$ are coprime and their product is a square, they are themselves squares, say $r=u^{2}, s=v^{2}$.

- then

$$
n^{2}=b=r^{2}+s^{2}=u^{4}+v^{4}
$$

- thus from our original solution $x, y, z$ we have produced a new solution $u, v, n$
- but notice $z=a^{2}+b^{2}=a^{2}+n^{4}$, so $n^{4}=z-a^{2}$, hence $n<z$.
- Thus we have our descent.
- To repeat from above, this is a contradiction because we cannot keep producing smaller and smaller positive integers.
- since given any positive integer solution $x, y, z$, we get the descent, there cannot be any positive integer solutions at all.


## 3. Other Examples of Descent

The method of descent is very useful. It's a little bit like mathematical induction, but backwards. It may not be quite as useful as induction, but is still a very useful problem-solving tool. Here are some more applications of this idea:

Example 3.1. Problem: Prove that the equation $x^{3}+2 y^{3}+4 z^{3}=0$ has no solutions in integers except the trivial solution $x=y=z=0$.

Solution: Suppose we have a nontrivial solution $x, y, z$. We will produce another solution $x^{\prime}, y^{\prime}, z^{\prime}$ with $\left|x^{\prime}\right|<|x|$. Since the absolute value of $x$ cannot decrease forever, this descent will provide a contradiction.

Since $x^{3}+2 y^{3}+4 z^{3}=0, x$ must be even, say $x=2 k$. Then dividing the equation by 2 gives

$$
y^{3}+2 z^{3}+4 k^{3}=0
$$

Now $y$ must be even, say $y=2 m$. Dividing by 2 again gives

$$
z^{3}+2 k^{3}+4 m^{3}=0
$$

so $z$ is even, say $z=2 n$. Dividing by 2 one last time, we get

$$
k^{3}+2 m^{3}+4 n^{3}=0
$$

But $|k|=|x| / 2<|x|$, so we have desecent, giving a contradiction.

Example 3.2. Problem: Show that if $d$ is not a perfect square, then $\sqrt{d}$ is an irrational number.

Solution: Suppose $d$ is rational. Let $a=\lfloor\sqrt{d}\rfloor$, and put $\sqrt{d}=a+\frac{b}{c}$, where $0<\frac{b}{c}<1$, so $0<b<c$. We will use descent on the denominator $c$. Squaring both sides of $\sqrt{d}=a+\frac{b}{c}$ and clearing the denominator gives

$$
d c^{2}=a^{2} c^{2}+2 a b c+b^{2}
$$

This shows that $c \mid b^{2}$, say $b^{2}=c n$. Then $\frac{b}{c}=\frac{n}{b}$, and this new fraction $\frac{n}{b}$ has smaller denominator. So we have a descent. Contradiction ${ }^{2}$.

Example 3.3. Problem: Prove that if $n>1, n$ does not divide $2^{n}-1$.
Solution: Suppose there is an integer $n>1$ such that $n \mid 2^{n}-1$. Then this $n$ has at least one prime factor $p$. We will produce a smaller prime factor. This is the descent, and it gives a contradiction, since we cannot keep producing smaller and smaller primes!

- So let $p \mid n$; then $p|n| 2^{n}-1$, so $2^{n} \equiv 1 \bmod p$.
- let $k$ be the order of $2 \bmod \mathrm{p}$.
- by def of order, $k \mid n$, and also since $2^{p-1} \equiv 1 \bmod p, k \mid p-1$.
- $k \neq 1$, because the only thing that has order $1 \bmod p$ is 1 . So there is a prime factor $q$ of $k$, which is therefore also a prime factor of $n$.
- But $q<p$, because $q$ divides $k$, which divides $p-1$.
- so we have our descent: given a prime factor $p$ of $n$, we get a prime factor $q$ of $n$ which is strictly smaller. This is a contradiction.

[^1]
[^0]:    ${ }^{1}$ Note: the following argument is a little different from the one in your book.

[^1]:    ${ }^{2}$ Notice that these denominators are positive, which is essential for the contradiction.

