# Math 4527 (Number Theory 2)

## Lecture #10 of 38 $\sim$ February 10, 2021

---

Miscellaneous Diophantine Equations

- Miscellaneous Diophantine Equations

This material represents §6.4 from the course notes.

# Miscellaneous Diophantine Equations, XVII

Example: Find all solutions to the Diophantine equation $3^a - 2^b = 1$.

# Miscellaneous Diophantine Equations, XVII

Example: Find all solutions to the Diophantine equation $3^a - 2^b = 1$.

- The idea of this result is to use congruence conditions.
- Clearly $a$ and $b$ must be nonnegative, else the denominators of the rational numbers involved could not be equal.
- Clearly $b = 0$ does not work, while $b = 1$ gives $a = 1$.
- Now suppose $b \geq 2$ and consider the equation modulo 4: we obtain $3^a \equiv 1 \pmod 4$, meaning that $a$ is even, say, $a = 2k$.
- Then we have $2^b = 3^{2k} - 1 = (3^k + 1)(3^k - 1)$, so $3^k + 1$ and $3^k - 1$ must both be powers of 2.
- But their difference is 2, and so they must be 4 and 2 respectively. Thus, the only other solution is $(a, b) = (2, 3)$.

# Miscellaneous Diophantine Equations, XVIII

This result is a special case of a result called Catalan's conjecture (proven in 2002 by Mihailescu) that 8 and 9 are the only perfect powers that are consecutive.

- In other words, the only solutions to $x^a - y^b = 1$ in integers greater than 1 is $(a, b, x, y) = (2, 3, 3, 2)$.
- In 1976, Tijdeman used results on linear forms in logarithms to show that any solution to $x^a - y^b = 1$ in integers greater than 1 would have to have $a, b$ below an (extremely large) finite bound, which established that there were only finitely many solutions.
- However, the bound was on the order of $e^{e^{e^{e^{730}}}}$, which is completely infeasible to check computationally.

# Miscellaneous Diophantine Equations, XIX

Example: Show that the Diophantine equation $y^2 = x^3 + 7$ has no solutions.

# Miscellaneous Diophantine Equations, XIX

Example: Show that the Diophantine equation $y^2 = x^3 + 7$ has no solutions.

- The idea of this result is to rewrite the equation slightly, exploit congruence conditions, and then quadratic reciprocity to obtain a contradiction.
- First, if $x$ is even, then this equation yields $y^2 \equiv 3 \pmod 4$, which is not possible.
- Thus, $x$ is odd and so $y$ is even. This requires $x^3 + 7 \equiv 0 \pmod 4$ so that $x^3 \equiv 1 \pmod 4$ and thus $x \equiv 1 \pmod 4$.
- Now we write the equation as $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$.
- To proceed further, we require a fact about divisors of integers of the form $n^2 + 1$:

# Miscellaneous Diophantine Equations, XX

**Proposition (Prime Divisors of $n^2 + 1$)**

*If $p$ is an odd prime and there is a solution to $y^2 \equiv -1 \pmod{p}$, then $p$ must be congruent to 1 modulo 4. Thus, every odd prime divisor of an integer of the form $n^2 + 1$ is congruent to 1 modulo 4.*

First note that $y^2 \equiv -1 \pmod{p}$ implies that $y$ has order 4 modulo $p$ (since $y^4 \equiv 1$ but no lower power can be 1 mod $p$). We now give two arguments for why this implies $p \equiv 1 \pmod{4}$.

1. Let $u$ be a primitive root $u$ modulo $p$. Then $u^r = a$ for some $r$, so $u^{4r} = 1$ and the order of $u$ cannot be smaller than $4r$. But since $u$ is a primitive root, its order equals the number of nonzero residues modulo $p$, which is $p - 1$.
2. By Lagrange's theorem, the order of any element in a group divides the order of the group. The group of nonzero residues modulo $p$ has order $p - 1$, and since there is an element of order 4, that means 4 divides $p - 1$.

# Miscellaneous Diophantine Equations, XXI

Example: Show that the Diophantine equation $y^2 = x^3 + 7$ has no solutions.

- Returning to our original problem, recall that we have shown that $x \equiv 1 \pmod 4$, and also that $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$.
- By the proposition, any odd prime divisor, and therefore *any* odd divisor (prime or otherwise), of $y^2 + 1 = x^3 + 8$ must be congruent to 1 modulo 4.
- But $x + 2$ is a divisor of $x^3 + 8$ congruent to 3 modulo 4, so we have a contradiction.
- Therefore, there are no solutions to the given Diophantine equation.

# Miscellaneous Diophantine Equations, XXII

Example: Show that the Diophantine equation $y^2 = x^3 + 7$ has no solutions.

- We remark that there is always a solution to the equation $y^2 = x^3 + 7$ modulo $p$ for every prime $p$. (We will essentially show this in a week or two when we discuss elliptic curves modulo $p$.)
- Thus, the natural approach of "reduce mod $p$ to try to find a contradiction" is not effective here.
- In fact (although this is much harder to prove!) there are not even any *rational* solutions to $y^2 = x^3 + 7$.
- As another (entirely irrelevant) remark, this elliptic curve was used in an early specification of the elliptic curve digital signature algorithm, and shows up in many practical implementations, including in the hashing signatures used by bitcoin.

# Miscellaneous Diophantine Equations, XXIII

Example: Show that there are infinitely many perfect squares that are the sum of two other consecutive perfect squares.

# Miscellaneous Diophantine Equations, XXIII

Example: Show that there are infinitely many perfect squares that are the sum of two other consecutive perfect squares.

- The idea of this result is to rearrange the equation and use properties of Pell's equation.
- Suppose that $a^2 = b^2 + (b+1)^2$ so that $a^2 = 2b^2 + 2b + 1$.
- Multiplying both sides by 2 and completing the square on the right-hand side yields $2a^2 = (2b+1)^2 + 1$, so that $(2b+1)^2 - 2a^2 = -1$.
- This is a Pell equation of the form $x^2 - 2y^2 = -1$, where $x = 2b + 1$.

# Miscellaneous Diophantine Equations, XXIV

Example: Show that there are infinitely many perfect squares that are the sum of two other consecutive perfect squares.

- Since the fundamental unit of $\mathbb{Z}[\sqrt{2}]$ is $u = 1 + \sqrt{2}$ which has norm $-1$, we know that $x^2 - 2y^2 = -1$ will have infinitely many solutions given by odd powers of $u$: $x + y\sqrt{2} = (1 + \sqrt{2})^{2k+1}$ for $k \geq 0$.
- Therefore, since $x$ is always odd in such solutions, each of these infinitely many solutions yields a different pair $(a, b)$ with $a^2 = b^2 + (b + 1)^2$.
- For example, the first few pairs $(a, b)$ are $(a, b) = (1, 0)$, $(5, 3)$, $(29, 20)$, $(169, 119)$, $(985, 696)$, $(5741, 4059)$, and so forth.

# Miscellaneous Diophantine Equations, XXIV

Example: Show that there are infinitely many perfect squares that are the sum of two other consecutive perfect squares.

- It is also possible to approach this problem using our characterization of the Pythagorean triples: the question is equivalent to having either $2st = s^2 - t^2 + 1$ or $2st = s^2 - t^2 - 1$, depending on whether $n$ is odd or even.
- Then, by completing the square, we see that this is equivalent to $(s - t)^2 - 2t^2 = \pm 1$, and so once again we are reduced to solving Pell's equation $x^2 - 2y^2 = \pm 1$.

# Miscellaneous Diophantine Equations, XXV

Example: Show that there are infinitely many noncongruent triangles whose side lengths are consecutive integers and whose area is also an integer.

# Miscellaneous Diophantine Equations, XXV

Example: Show that there are infinitely many noncongruent triangles whose side lengths are consecutive integers and whose area is also an integer.

- Suppose the side lengths are $d-1$, $d$, and $d+1$. Then by Heron's formula[1], we have $s = 3d/2$ so the area is given by $$A = \sqrt{\frac{3d}{2} \cdot \frac{d-2}{2} \cdot \frac{d}{2} \cdot \frac{d+2}{2}} = \frac{d\sqrt{3(d^2-4)}}{4}.$$
- Then we see $d$ must be even, say with $d = 2x$, and then $A = x\sqrt{3(x^2-1)}$, which is integral precisely when $3(x^2-1)$ is a perfect square.
- This perfect square must be a multiple of 3, so if $3(x^2-1) = (3y)^2$, we see $x^2 - 3y^2 = 1$.

[1] The area of a triangle with side lengths $a, b, c$ is equal to $K = \sqrt{s(s-a)(s-b)(s-c)}$ where $s = (a+b+c)/2$ is the semiperimeter

# Miscellaneous Diophantine Equations, XXVI

Example: Show that there are infinitely many noncongruent triangles whose side lengths are consecutive integers and whose area is also an integer.

# Miscellaneous Diophantine Equations, XXVI

Example: Show that there are infinitely many noncongruent triangles whose side lengths are consecutive integers and whose area is also an integer.

- Thus, the side lengths are $d-1$, $d$, and $d+1$ where $d=2x$ and $x^2-3y^2=1$. The area is then $x\sqrt{3(x^2-1)}=3xy$.
- Since the fundamental solution of this Pell's equation is $2+\sqrt{3}$, we see that there are infinitely many such $n$, obtained from the powers $x_n+y_n=(2+\sqrt{3})^n$.
- The first few such triangles (for $j=1,2,3,4$) are 3-4-5 (area 6), 13-14-15 (area 84), 51-52-53 (area 1170), and 193-194-195 (area 16296).

# The Fermat Equation $x^n + y^n = z^n$, I

One of the most famous Diophantine equations is Fermat's equation $x^n + y^n = z^n$, for a fixed integer $n \geq 3$.

- Clearly, there are solutions if one of the variables is equal to 0: the question is whether this equation possesses any other solutions.
- It is enough to prove the nonexistence of nontrivial solutions in the cases $n = 4$ and $n = p$ where $p$ is an odd prime, since any $n > 2$ is divisible by 4 or an odd prime.

# The Fermat Equation $x^n + y^n = z^n$, II

This result was famously conjectured by Fermat in 1637, who wrote (in the margin of his book, in Latin) "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain."

- It is now believed that Fermat probably did not have a correct proof of this result.
- As we will discuss more in later chapters, a substantial amount of number theory and abstract algebra was developed in the mid-19th and early-20th centuries in an attempt to establish the nonexistence of nontrivial integer solutions to $x^n + y^n = z^n$.

# The Fermat Equation $x^n + y^n = z^n$, III

One of the easier cases is $n = 4$, which is in fact the subject of one of Fermat's very few theorems for which he gave an actual proof:

**Theorem (Fermat's Theorem)**

*The Diophantine equation $x^4 + y^4 = z^2$ has no solutions with $xyz \neq 0$. In particular, $x^4 + y^4 = z^4$ has no nontrivial solutions.*

We show the result using a technique equivalent to induction that is often called Fermat's method of infinite descent, which in fact first appeared in the proof of this very result.

- The idea is to consider the smallest nontrivial solution of the equation in positive integers and use it to construct a smaller solution: the well-ordering principle of the integers then yields a contradiction, since we cannot have an infinite decreasing sequence of positive integers.

# The Fermat Equation $x^n + y^n = z^n$, IV

Proof:

- Suppose the equation has nontrivial solutions and let $u$ be the smallest positive integer such that $x^4 + y^4 = u^2$ has a solution.
- Observe that $\gcd(x, y) = 1$, otherwise we could replace $x, y, u$ with $x/d$, $y/d$, $u/d^2$ to obtain a smaller solution.
- By reducing both sides modulo 4, we see that one of $x, y$ is even and the other is odd: without loss of generality, assume $x$ is even.
- Then $(x^2, y^2, u)$ is a primitive Pythagorean triple, so from our parametrization we see that $x^2 = 2st$, $y^2 = s^2 - t^2$, and $u = s^2 + t^2$ for some integers $s > t > 0$ of opposite parity.

# The Fermat Equation $x^n + y^n = z^n$, V

Proof:

- We have $x^2 = 2st$, $y^2 = s^2 - t^2$, and $u = s^2 + t^2$ for some integers $s > t > 0$ of opposite parity.
- Since $y^2 = s^2 - t^2$, it must be the case that $s$ is odd and $t$ is even: otherwise, $y^2 = s^2 - t^2$ would be $-1$ modulo 4.
- If we set $t = 2k$, we see $(x/2)^2 = sk$ where $\gcd(s, k) = 1$, so both $s$ and $k$ are perfect squares by the uniqueness of prime factorizations.
- Setting $s = a^2$ and $k = b^2$ yields the system $y^2 = s^2 - t^2 = a^4 - 4b^4$, so that $y^2 + (2b^2)^2 = a^4$.

# The Fermat Equation $x^n + y^n = z^n$, VI

Proof:

- We have $x^2 = 2st$, $y^2 = s^2 - t^2$, and $u = s^2 + t^2$, where $t = 2k$, $s = a^2$ and $k = b^2$.
- Since $y^2 + (2b^2)^2 = a^4$, this means $(y, 2b^2, t)$ is also a primitive Pythagorean triple, so there exist relatively prime integers $m$ and $n$ such that $2b^2 = 2mn$, $y = m^2 - n^2$, and $a^2 = m^2 + n^2$.
- The first equation gives $b^2 = mn$, so $m$ and $n$ are both squares: say, $m = v^2$ and $n = w^2$.
- Then, at last, we see that $a^2 = v^4 + w^4$, meaning that we have a new solution $(v, w, a)$ to the original equation. Clearly $a \leq a^2 = s < s^2 + t^2 = u$, so this solution is smaller.
- This is a contradiction since we started with the smallest solution, so there are no nontrivial solutions to $x^4 + y^4 = u^2$.

# The Fermat Equation $x^n + y^n = z^n$, VII

We can use an approach similar to the factorization-in-$\mathbb{Z}[i]$ procedure to handle the case where $n = 3$.

- The idea is to factor the equation $x^3 + y^3 = z^3$ in the ring $\mathbb{Z}[\rho]$, where $\rho = (1 + \sqrt{-3})/2$ is a non-real cube root of unity.
- The elements of this ring are of the form $a + b\rho$ for $a, b \in \mathbb{Z}$, (this is in fact a ring because $\rho^2 = -\rho - 1$).
- It can be shown that $\mathbb{Z}[\rho]$ has unique factorization (we will in fact prove this later in the semester), so inside $\mathbb{Z}[\rho]$, we can factor $x^3 + y^3 = z^3$ as $(x + y)(x + \rho y)(x + \rho^2 y) = z^3$.
- Now the idea is to show that, up to small factors, the terms $x + y$, $x + \rho y$, $x + \rho^2 y$ are relatively prime in $\mathbb{Z}[\rho]$.
- Up to these small factors, each of these terms must therefore be a perfect cube, but this cannot actually occur. (The precise details are rather lengthy and technical, so we will skip them for now.)

# The Fermat Equation $x^n + y^n = z^n$, VIII

The argument in the $n = 3$ case lends itself to a natural generalization, namely, factoring $x^n + y^n = z^n$ over the ring $\mathbb{Z}[\zeta_n]$ where $\zeta_n = e^{2\pi i/n}$ is an $n$th root of unity.

- However, quite unfortunately, for most $n$, the ring $\mathbb{Z}[\zeta_n]$ does not have unique factorization!
- So (alas!) this technique does not work in general.
- However, determining when this approach can succeed was one of the original historical motivations for studying unique factorization in general rings.

# The Fermat Equation $x^n + y^n = z^n$, X

The cases $n = 5$ and $n = 7$ were shown in the 1800s by various mathematicians using various techniques.

- A number of other cases were shown individually, and then results of Germain and others established infinite classes of prime $n$ for which there are no nontrivial solutions to the equation.
- However, the lack of a solution to Fermat's equation for every $n > 2$ was not established until 1995, with Andrew Wiles's celebrated proof of the Taniyama-Shimura-Weil conjecture. (Wiles announced his result in 1993, but a gap was discovered later that year. Wiles, working with Richard Taylor, closed the gap by 1994.)

# The Fermat Equation $x^n + y^n = z^n$, XI

One of the initial steps in Wiles's proof stemmed from an observation made by Frey in 1984, which connects the solutions to $a^p + b^p = c^p$ to a certain elliptic curve.

- Such a curve would have a number of unusual properties, and (in particular) is what is called a semistable elliptic curve, and it would also fail to be modular.
- Wiles's results proved that every semistable elliptic curve is modular, which, when combined with Frey's observations, shows that the Fermat equation cannot have a solution in nonzero integers.
- Over the next few chapters, we will develop more of the background necessary to understand this result. But we will close by noting that, as with most major mathematical advances, the fundamental ideas put forward in Wiles's work are just as important as the end result of his proof.

# Summary

We discussed some more miscellaneous Diophantine equations and some methods for solving them.

We discussed Fermat's equation $x^n + y^n = z^n$.

Next lecture: Elliptic curves and the group law.