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, I

Our goal now is to give a roundup of a bunch of miscellaneous Diophantine equations and discuss some methods for solving them.

- As I said in the first lecture, there is no general procedure for solving an arbitrary Diophantine equation.
- As such, the methods we use tend to feel a bit *ad hoc*, since there are very many different things one may try to solve these equations.
- The goal is to mention most of the more standard sorts of techniques (using modular arithmetic, descent arguments, factorization in $\mathbb{Z}$ or in $\mathbb{Z}[\sqrt{D}]$, exploiting inequalities, etc.) and illustrate their applications via example.

Miscellaneous Diophantine Equations, II

Example: Solve the Diophantine equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{2021}$ in positive integers (x, y).

Miscellaneous Diophantine Equations, II

Example: Solve the Diophantine equation $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{2021}$ in positive integers (x, y).

- The idea here is to rearrange the equation and factor.
- Note that $x, y \geq 2022$.
- Clearing denominators yields $2021y + 2021x = xy$, so that $xy - 2021x - 2021y = 0$.
- Adding 2021^2 to both sides then allows us to factor this equation as $(x - 2021)(y - 2021) = 2021^2$.
- Since $x, y \geq 2022$ we can then simply find the possible factorizations of 2021^2 as a product of two positive integers.

Miscellaneous Diophantine Equations, III

Example: Solve the Diophantine equation $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{2021}$ in positive integers (x, y).

Miscellaneous Diophantine Equations, III

Example: Solve the Diophantine equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{2021}$ in positive integers (x, y).

- With $(x - 2021)(y - 2021) = 2021^2$, we can see that $2021^2 = 43^2 \cdot 47^2$ has 9 possible factorizations as the product of two positive integers, 5 of which correspond to having $x \geq y$: $1 \cdot 2021^2$, $43 \cdot (43 \cdot 47^2)$, $47 \cdot (43^2 \cdot 47)$, $2021 \cdot 2021$.
- These factorizations yield five possible pairs $(x - 2021, y - 2021) = (1, 4084441)$, $(43, 94987)$, $(47, 86903)$, $(1849, 2209)$, $(2021, 2021)$.
- Thus we get the solutions $(x, y) = (2022, 4086462)$, $(2064, 97008)$, $(2068, 88924)$, $(3870, 4230)$, and $(4042, 4042)$.

Miscellaneous Diophantine Equations, IV

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b + 7)$.

Miscellaneous Diophantine Equations, IV

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b + 7)$.

- The idea of this proof is to use modular arithmetic and induction on a. Clearly, $a \geq 0$.
- For the base case $a = 0$, consider the equation modulo 8.
- Each of the squares x^2, y^2, and z^2 is either 0, 1, or 4 mod 8, so it is not possible to obtain a sum of 7 mod 8 by adding three of them.
- Therefore, there are no solutions to $x^2 + y^2 + z^2 = 8b + 7$.

Miscellaneous Diophantine Equations, V

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b+7)$.

Miscellaneous Diophantine Equations, V

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b+7)$.

- For the inductive step, now suppose there are no solutions for $a \leq k$, and take $a = k+1$.
- Consider the equation $x^2 + y^2 + z^2 = 4^{k+1}(8b+7)$ modulo 4.
- Each of the squares is 0 or 1, while the term $4^{k+1}(8b+7)$ is 0 mod 4, so all of the squares must be 0 mod 4.
- Then $(x/2)^2 + (y/2)^2 + (z/2)^2 = 4^k(8b+7)$, but by the inductive hypothesis, this equation has no solutions.
- Therefore there are no solutions for $a = k+1$ either, so by induction, there are no solutions for any a.

Miscellaneous Diophantine Equations, VI

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b + 7)$.

Miscellaneous Diophantine Equations, VI

Example: Show that there are no solutions to the Diophantine equation $x^2 + y^2 + z^2 = 4^a(8b + 7)$.

- In fact, these are the only integers that cannot be written as a sum of three squares, as first proven by Legendre.
- Gauss gave a formula for the number of such representations, similar to Fermat's formula for the number of ways of writing an integer as a sum of two squares.
- We will prove this characterization of sums of three squares (along with sums of two squares and sums of four squares) later in the semester.

Miscellaneous Diophantine Equations, VII

Example: Find all of the solutions to the Diophantine equation $y^2 = x^4 + 4x^3 + x^2 + 2x + 1$.

Miscellaneous Diophantine Equations, VII

Example: Find all of the solutions to the Diophantine equation $y^2 = x^4 + 4x^3 + x^2 + 2x + 1$.

- The idea of this result is to attempt to complete the square of the x-terms, and then use some simple inequalities to bound how big x and y can be.
- We complete the square of the x-terms and obtain $x^4 + 4x^3 + x^2 + 2x + 1 = \left(x^2 + 2x - 3/2\right)^2 + (8x - 5/4)$.
- If x is large then this tells us that $\sqrt{x^4 + 4x^3 + x^2 + 2x + 1} \approx x^2 + 2x - 3/2$, which is between the two integers $x^2 + 2x - 2$ and $x^2 + 2x - 1$.
- Thus, we can bound $|x|$ by comparing $x^4 + 4x^3 + x^2 + 2x + 1$ to the squares $(x^2 + 2x - 2)^2$ and $(x^2 + 2x - 1)^2$.

Miscellaneous Diophantine Equations, VIII

Example: Find all of the solutions to the Diophantine equation $y^2 = x^4 + 4x^3 + x^2 + 2x + 1$.

Miscellaneous Diophantine Equations, VIII

Example: Find all of the solutions to the Diophantine equation $y^2 = x^4 + 4x^3 + x^2 + 2x + 1$.

- First, we have $y^2 - (x^2 + x - 2)^2 = x^2 + 10x - 3$. This quadratic is positive outside the interval $[-10.3, 0.3]$.
- Likewise, we also see that $(x^2 + x - 1)^2 - y^2 = x^2 - 6x$ is positive outside $[0, 6]$.
- Hence, if $x \notin [-10, 6]$, then we have the strict inequalities $(x^2 + x - 2) < y^2 < (x^2 + x - 1)^2$, which is impossible if x and y are both integers.
- Now we just have to check the 17 possible integers x, namely, $x = -10, -9, \ldots, 6$ to see which ones yield an integral value of y.
- This is not hard to do by hand but it's even easier via computer. This will show the solutions are $(x, y) = (-4, \pm 3)$, $(0, \pm 1)$, $(1, \pm 3)$, and $(6, \pm 47)$.

Miscellaneous Diophantine Equations, IX

A few remarks about the more general Diophantine equation $y^2 = q(x)$ where $q(x)$ is a polynomial with integer coefficients:

- In degree 1, there are infinitely many solutions unless there is some modular-arithmetic constraint (e.g., $y^2 = 4x + 3$).
- In even degrees, one can adapt the proof method we just used to show that there are only finitely many solutions for any monic polynomial $q(x) \in \mathbb{Z}[x]$ that is not a perfect square.
- Of course, if $q(x)$ is a perfect square, then $y^2 = q(x)$ will clearly have infinitely many solutions (any x will work!).
- If $q(x)$ is not monic, the question is more subtle, since for example, $y^2 = 3x^2 + 1$ has infinitely many solutions, while $y^2 = 3x^2 - 1$ has none. In general, in degree 2, any such equation can be converted into a conic and analyzed using the tools we have developed for Pell's equation.

Miscellaneous Diophantine Equations, X

One can also study the more general Diophantine equation $y^2 = q(x)$ where $q(x)$ is a polynomial with integer coefficients.

- In degree ≥ 3 there are only finitely many integral solutions: this is a result known as Siegel's theorem.
- Even in the situation where q is monic of degree 3, the situation is quite complicated: such equations $y^2 = x^3 + ax^2 + bx + c$ yield elliptic curves, which is the topic of our next chapter.
- A much stronger result was proven by Faltings. A special case of this result implies that if $\deg q \geq 5$ and q is a squarefree polynomial, then in fact there are only finitely many rational solutions to $y^2 = q(x)$.

Miscellaneous Diophantine Equations, XI

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

Miscellaneous Diophantine Equations, XI

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

- The idea of this proof is first to exploit the arithmetic of the Gaussian integers $\mathbb{Z}[i]$.
- So suppose x, y are relatively prime. If x, y were both odd, then we would have $z^3 \equiv 2 \pmod 4$, but 2 is not a cube modulo 4.
- Since x, y are not both even since $\gcd(x, y) = 1$, we conclude that one is even and the other is odd.
- Now, over $\mathbb{Z}[i]$, factor the equation as $(x + iy)(x - iy) = z^3$.
- We claim that $x + iy$ and $x - iy$ are relatively prime: any common divisor would divide both $2x$ and $2y$, hence divide 2. But $1 + i$ (the only Gaussian prime dividing 2) does not divide $x + iy$, since x, y are of opposite parity.

Miscellaneous Diophantine Equations, XII

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

Miscellaneous Diophantine Equations, XII

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

- Thus, $x + iy$ and $x - iy$ are relatively prime, and their product is a perfect cube.
- By the uniqueness of prime factorization in $\mathbb{Z}[i]$, we conclude that $x + iy$ must be a unit times a cube.
- But since each unit in $\mathbb{Z}[i]$ is actually a cube, we conclude that $x + iy = (a + bi)^3$ for some $a + bi \in \mathbb{Z}[i]$.
- Equating real and imaginary parts yields $x = a^3 - 3ab^2$, $y = 3a^2b - b^3$, and then $z = (a + bi)(a - bi) = a^2 + b^2$.

Miscellaneous Diophantine Equations, XIII

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

Miscellaneous Diophantine Equations, XIII

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

- If x, y are not relatively prime, there are additional solutions.
- To see how these arise, suppose p is an integer prime dividing both x, y. Then $p^2 | z^3$ so $p | z$.
- Setting $x = px'$, $y = py'$, $z = pz'$ then yields $(x')^2 + (y')^2 = p(z')^2$.
- If we again factor over $\mathbb{Z}[i]$ we see that $p | (x' + iy')(x' - iy')$.
- If p is irreducible in $\mathbb{Z}[i]$, which occurs whenever $p \equiv 3 \pmod 4$, then in fact p would have to divide one term (and thus by conjugating it would divide the other) which by repeating the argument would force $p^3 | x$, $p^3 | y$, and $p^2 | z$. We could then pull out the factors of p and solve the reduced equation $(x/p^3)^2 + (y/p^3)^2 = (z/p^2)^3$.

Miscellaneous Diophantine Equations, XIV

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

Miscellaneous Diophantine Equations, XIV

Example: Solve the Diophantine equation $x^2 + y^2 = z^3$ for $\gcd(x, y) = 1$.

- However if p factors in $\mathbb{Z}[i]$ as $\pi\overline{\pi}$, which occurs for $p = 2$ and for $p \equiv 1 \pmod 4$ we could then have $x' + iy' = \pi \cdot w$ with $x' - iy' = \overline{\pi} \cdot \overline{w}$, where now $w\overline{w} = z^3$.
- These yield additional solutions upon expanding out the real and imaginary parts.
- For example, taking $p = 5 = (2 + i)(2 - i)$, so that $\pi = 2 + i$, yields solutions $x + iy = 5(2 + i)(a + bi)^3$ so that $(x, y) = (10a^3 - 15a^2b - 30ab^2 + 5b^3, 5a^3 + 30a^2b - 15ab^2 - 10b^3)$.

Miscellaneous Diophantine Equations, XV

Example: Show that the only solution to the Diophantine equation $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.

Miscellaneous Diophantine Equations, XV

Example: Show that the only solution to the Diophantine equation $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.

- Clearly, $\gcd(x, y) = 1$ since any common divisor would also divide $y^2 - x^3 = -1$.
- Now, rearranging the equation into the form $1 + y^2 = x^3$ and applying the previous result shows that $1 = a^3 - 3ab^2$ for $a, b \in \mathbb{Z}$.
- Factoring gives $1 = a(a^2 - 3b^2)$.
- Clearly, $a \in \pm 1$, and then the only solution is easily seen to be $(a, b) = (1, 0)$, yielding $(x, y) = (1, 0)$.

Miscellaneous Diophantine Equations, XVI

Example: Find all solutions to the Diophantine equation $7^a - 4^b = 3$.

Miscellaneous Diophantine Equations, XVI

Example: Find all solutions to the Diophantine equation $7^a - 4^b = 3$.

- The idea of this result is to use congruence conditions.
- Clearly a and b must be nonnegative, since otherwise 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 8: we obtain $7^a \equiv 3 \pmod 8$.
- However, there are no solutions to this equation, because 7^a can only be 7 or 1 modulo 8.
- Therefore, the only solution is $(a, b) = (1, 1)$.

Summary

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

Next lecture: Miscellaneous Diophantine equations (part 2).