Diophantine Equations

James Rickards
jamesarickards@hotmail.com

1 Introduction

A classic number theory problem takes the form

Find all (positive) integer/rational solutions to the following equation/inequality

Such a question is called a Diophantine equation. Despite the area being thousands of years old (it's roots being the irrationality of $\sqrt{2}$), it is still one of the top current research topics.

As with most of math, there is no single method that will solve all Diophantine equations. If you write down a completely random equation, it's fairly likely to be quite easy or not possible to solve with elementary techniques.

2 Strategies

Here are some basic strategies and tips to remember:

- Search for small solutions: if there are non-trivial ones, this may be worth a point if you get them all;
- Look modulo primes/prime powers to deduce information about the variables;
- Try to rearrange and factor terms; show that such factors have bounded gcd;
- Rewrite equations involving squares, look for squares with a small difference between them;
- Bound the sizes of different variables;
- Sometimes casework is needed, get comfortable of when. Sometimes casework devolves into more casework and will never end, and sometimes it doesn't: it's good to have intuition about if your casework is useful or not.

Some simple examples are:

Example 1. *Find all integer solutions to* $y^2 = x^5 + 7$.

Solution. Modulo 11, the possible fifth powers are $-1, 0, 1$. Thus $y^2 \equiv 6, 7, 8 \pmod{11}$, and these are all not quadratic residues modulo 11. Thus there are no solutions. □

Example 2. *Find all positive integer solutions to* $y^2 = (x^2 + 1)(2x^2 + 6)$.

Solution. The gcd of the right hand side divides $(2x^2+6)-2(x^2+1)=4$, so it is $1,2,4$. Thus we either have $x^2+1, 2x^2+6$ being both squares, or twice squares. In the first case, we let $(x^2+1, 2x^2+6) = (a^2, b^2)$, so then $a^2 - x^2 = 1$. Thus $a > x$, and write $a = x + r$ with $r > 0$ an integer. Thus $1 = r^2 + 2rx \geq 1 + 2 = 3 > 1$, contradiction.
Otherwise, $(x^2+1, 2x^2+6) = (2a^2, 2b^2)$, whence $b^2 - x^2 = 3$. As above, $b = x + r$ for $r > 0$, whence $3 = r^2 + 2xr \geq 1 + 2 = 3$, with equality iff $r = x = 1$. This gives rise to $(x, y) = (1, 4)$, which is thus the only solution. □

3 Two Variable Polynomials

Let $f(x, y)$ be a two variable integer polynomial, and consider the equation $f(x, y) = 0$ to be solved in the rational numbers. For a generic such equation, we can assign it a non-negative integer g, called the genus. For example, the curves:

1. $x^2 + y^2 = 1$ has genus 0
2. $y^2 = x^3 + x + 1$ has genus 1
3. $y^2 = x^5 + x$ has genus 2

A genus zero curve will have a family of solutions which can be solved easily. For example,

Example 3. *Find all rational solutions to* $x^2 + y^2 = 1$.

Solution. If $x = 1$ then $y = 0$ necessarily. Next starting with the rational solution $(1, 0)$, the general equation of a line with rational slope through this point is $y = tx - t$ for any rational number t. Plugging this in to our original equation, we have $(t^2+1)x^2 - 2t^2x + t^2 - 1 = 0$. But we know that $x = 1$ is a solution, so this quadratic must factor! The solutions multiply to $x = \frac{t^2-1}{t^2+1}$, hence this is the other root. But all rational solutions can be constructed in this manner, as the line through the solution and $(1, 0)$ will have finite rational slope. Thus the solution set is

$$(x, y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right), (1, 0)$$

for any rational t. □

A genus 1 curve can have either finitely or infinitely many solutions, and such an equation is called an Elliptic Curve. Studying these equations is one of the hottest topics in current number theory, and they are still very mysterious. If one of these equations appears on a contest, then it will most likely have finitely many solutions, as there is no elementary (high school level) way to describe the infinite families of solutions.

Finally, a curve of genus at least 2 has finitely many rational solutions by Faltings's theorem. So you could eventually find all solutions by ordering all possible (x, y) values and checking them, but you will have no way of knowing if you've found them all or need to search more...

4 Local Global Principle

If $f(x_1, \ldots, x_n)$ is an integer polynomial, then $f = 0$ having an integer solution will imply that there is a solution in $\mathbb{R}$ and modulo p for all primes p. The opposite implication is very closely related to something called the "local-global principle." This principle holds if f is a quadratic polynomial, but does not hold in generality. For example,

$$(x^2 - 2)(x^2 - 3)(x^2 - 6) = 0$$

has solutions in $\mathbb{R}$ and modulo all primes p, but no solution in $\mathbb{Q}$.
Even though the principle does not always hold, looking modulo p is still very useful.

5 A Couple Useful Theroems

Theorem 1 (Lifting the exponent lemma)**.** *Let p be prime, x, y integers, and n a positive integer such that $p \mid x - y$ and $p \nmid x, y$. Then we have*

- *If p is odd, then*
$$v_p(x^n - y^n) = v_p(x - y) + v_p(n);$$
- *If $p = 2$, then*
$$v_2(x^n - y^n) = v_2(x - y) + v_2(n) + v_2(x + y) - 1.$$

Lifting the exponent (LTE) can be proved by induction (useful exercise!), and can be quite useful.

Theorem 2 (Zsigmondy's Theorem)**.** *Let $a > b > 0$ be coprime positive integers. Given an integer $n \geq 1$, there exists a primitive prime divisor of $a^n - b^n$, i.e. a prime p such that $p \mid a^n - b^n$ but $p \nmid a^k - b^k$ for all $1 \leq k \leq n - 1$, except in the following cases:*

- *$n = 1$, $a - b = 1$ (there are no prime factors);*
- *$n = 2$, $a + b$ is a power of 2;*
- *$n = 6$, $a = 2$, $b = 1$.*

Exercise 1. *Prove Zsigmondy's Theorem (or just the special case of $a = 2, b = 1$) using lifting the exponent lemma and bounding (if all prime factors came from previous terms, we can use LTE to know exactly how much they contribute, and can show that there is not enough there).*

Zsigmondy's Theorem is very powerful and is often overkill, but it has its uses.

Corollary 1. *Given any integer $a > 1$ and any $n \neq 2, 6$, there is a prime p for which a has order n modulo p (and of course $n = 2, 6$ will work in all but the exceptional cases described above).*

Corollary 2. *$2^n + 1$ has a prime divisor that is at least as big as $2n + 1$ for all $n \neq 3$.*

6 Problems

I will adopt the David Arthur style of ordering problems into 3 sections: A,B,C. A-level problems should be approximately CMO level, B level problems would be easy-medium IMO problems, and C level would be medium-hard IMO or beyond problems. This ordering is of course somewhat subjective, so don't be surprised if you find some problems to be out of place.

A1. Find the number of ordered pairs of positive integer solutions (m, n) to the equation $20m + 12n = 2012$.

A2. Find the positive integer n such that $n^{13} = 2198214591730833048701369$.

A3. Given that $34! = 295232799cd960414084761860964 35ab000000$ in base 10, find a, b, c, d.

A4. Find all positive rational solutions (x, y) to $x^2 + 3y^2 = 1$.

A5. Find all integers a such that $x^3 - x + a$ has three integer roots.

A6. Find the positive integer n such that $n^5 = 133^5 + 110^5 + 84^5 + 27^5$.

A7. Find all integer solutions (x, y) to $x^3y^2(2y - x) = x^2y^4 - 36$.

A8. Show that $|12^m - 5^n| \geq 7$ for all positive integers m, n.

A9. Find all integer solutions to $6(6a^2 + 3b^2 + c^2) = 5n^2$.

B1. Determine all pairs of rational numbers (x, y) such that $x^3 + y^3 = x^2 + y^2$.

B2. Find all pairs (x, y) of integers which satisfy $y^2 = x^3 + 16$.

B3. Find the integer solutions to $y^3 = 3x^2 + 3x + 7$.

B4. Find all triples (a, b, c) of positive integers such that $a!b! = a! + b! + c!$.

B5. Find all integer triples (a, b, c) with $a > 0 > b > c$ and $a + b + c = 0$ such that $2017 - a^3b - b^3c - c^3a$ is a perfect square.

B6. Find all pairs (m, n) of non-negative integers such that $m^2 + 2 \cdot 3^n = m(2^{n+1} - 1)$.

B7. Prove there are unique positive integers a, n such that $a^{n+1} - (a + 1)^n = 2001$.

B8. Find all pairs of positive integers (m, n) satisfying $3^m - 7^n = 2$.

B9. Let a, b, c be positive integers such that $\gcd(a, b) = 1$ and c is coprime to at least one of a, b. Prove that there exist infinitely many triples (x, y, z) of distinct positive integers such that $x^a + y^b = z^c$.

C1. Find all *positive* integers N such that $x^2 + y^2 + N(xy + 1) = 0$ has an integer solution (x, y).

C2. Find all *positive* integers N such that $x^2 + y^2 - Nxy + 1 = 0$ has a positive integer solution (x, y).

C3. Find all integer solutions to $\frac{x^7-1}{x-1} = y^5 - 1$.

C4. Find all non-negative integer solutions (x, y, z, w) to the equation $2^x 3^y - 5^z 7^w = 1$.

C5. Find all pairs of positive integers $m, n \geq 3$ such that there are infinitely many positive integers a such that $\frac{a^m+a-1}{a^n+a^2-1}$ is an integer.

C6. Integers $x > 2$,$y > 1$,$z > 0$ satisfy $x^y + 1 = z^2$. If $\omega(n)$ denotes the number of distinct prime divisors of n, prove that $\omega(x) \geq \omega(y) + 2$.

C7. Show that there are infinitely many pairs (x, y) of rational numbers such that $x^3 + y^3 = 9$.

C8. Show that there are no positive integer solutions (x, y) to $(x + 1)(x + 2) \cdots (x + 2014) = (y + 1)(y + 2) \cdots (y + 4028)$.

C9. Solve $x^2 + 7 = 2^n$ in the integers.

7 Hints

A1. Use mods.

A2. Look mod 10, approximate the number.

A3. Find max power of 10 dividing 34!, then look at the rest mod $9, 10, 11$.

A4. Look at the example from the lecture and emulate it.

A5. Use Vieta's formulas.

A6. Look modulo small primes and bound n.

A7. Rearrange to $36 = (xy(x-y))^2$, and do some casework (many solutions!).

A8. If not show that $|12^m - 5^n| = 1$, and rule this out modulo 11.

A9. Look modulo $2, 3$ and get an infinite descent argument so show only $a = b = c = n = 0$ works.

B1. Write $x = yk$ for k rational (and don't forget about the case of $y = 0$).

B2. Bring 16 to the left hand side and factor.

B3. Show that $y \equiv 1 \pmod 3$ and then look modulo 9.

B4. Try small cases to find the one solution. Assume $c \geq b \geq a$ and divide by $a!$, look modulo n for appropriate n.

B5. Sub in for c, simplify and factor to get the equation $a^2 + ab + b^2 = N$; solve this.

B6. Solve for m, get a new equation involving only n. Look modulo various primes or use lifting the exponent lemma to finish.

B7. Look modulo $a, a+1$ to pin down a, and then find the unique n.

B8. Look at the equations modulo good choices of primes when $n \geq 2$ or $m \geq 3$.

B9. There are in fact solutions with $x^a = y^b$, try with this simplification.

C1. $N = 5$ is the only N, try Vieta jumping/polynomial division.

C2. $N = 3$ is the only N, try Vieta jumping/polynomial division.

C3. Recall the lemma: prime divisors of $\frac{x^p-1}{x-1}$ (p is a prime) are all 0 or 1 modulo p.

C4. There are four solutions. You can solve pretty much the whole problem with modular arithmetic.

C5. Think in terms of polynomials, and play around with the algebra. There is one pair (m, n) that works.

C6. Manipulate to obtain the equation $\frac{a^y}{4} - b^y = \pm 1$, and recall the lemma that $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$.

C7. Try substituting $x = \frac{a+b}{2}$ and $y = \frac{a-b}{2}$. After another inversion/rescaling get an equation of the form $A^2 = B^3 + c$ for some constant c, and show this has infinitely many solutions by using two solutions to construct a third (this is an elliptic curve with rank at least 1).

C8. Show that x has to be quite large, and bound x between two quadratics in y.

C9. The possible n are $n = 3, 4, 5, 7, 15$. Do the n even case, and for n odd factorize in $\mathbb{Q}(\sqrt{7})$ (this is really beyond the level of olympiads, unless there is an alternate solution)