Diophantine Equations (Black Group)

Po-Ru Loh

June 25, 2010

The Hammers

When attacking a problem that falls into a well-defined category such as Diophantine equations, it can be very helpful to keep in mind a toolbox of different methods that commonly come in handy. Having such a list of tools can both help you make good use of time—reminding you to move on to other approaches when stuck on one—and suggest solution ideas that may be cleverly hidden from the surface. Here are some techniques to either refresh your memory or augment your arsenal.

1. **Modular analysis.** Taking mods is probably the first method most people learn for proving unsatisfiability of Diophantine equations. While some easier problems fall immediately to this approach, most olympiad problems use modular analysis only as a first step (if at all): indeed, any Diophantine equation with at least one solution will have solutions mod anything! Nonetheless, you might still find out that, say, $x \equiv 1 \pmod 3$ and then substitute $x = 3y + 1$ en route to a solution. One additional point worth mentioning is that the choice of modulus is not typically unmotivated: common tricks include modding out by coefficients or variables (to make terms vanish) or by primes p such that exponents appearing in the equation divide $p - 1$ (so that the number of possible residues is small). One memorable example involves a mixed cubic and quartic Diophantine equation that turns out to have no solutions mod 13—a seemingly random modulus at first glance, but in reality not so!

2. **Factorization.** The idea here is to perform some algebraic manipulation to convert one or both sides into a product of two or more factors; then, knowledge about prime factors on one side can be leveraged to deduce information about the factors on the other side. A good example—and useful trick in its own right!—is **Pythagorean substitution**, which characterizes the primitive Pythagorean triples $x^2 + y^2 = z^2$. Assuming that y and z are odd, we may write $y^2 = (z+x)(z-x)$ and use coprimality of the latter two factors to deduce that each must be a square; thus, we find $x = (r^2 - s^2)/2$, $y = rs$, and $z = (r^2 + s^2)/2$ for odd, coprime r, s. FIX THIS! Usually we instead take r, s to have opposite parity and substitute $r^2 - s^2$, $2rs$, and $r^2 + s^2$. Conversely, all such pairs r, s produce primitive Pythagorean triples.

3. **Inequalities.** Although talk of inequalities may seem odd in the context of Diophantine *equations*, much Diophantine analysis relies on bounding expressions in order to use the simple but critical facts that the integers are discrete and ordered—as opposed to the reals! (In contrast, the previous two methods made use of even spacing and unique prime factorization, respectively.) Two general approaches that fall into this category are **sandwiching integral expressions between consecutive integers** and **bounding the sizes of equal quantities** (often factors).

4. **Quadratic techniques.** The case of quadratics deserves special mention because of its popularity and the sizable number of special techniques tailored to it.

   - First, the **quadratic formula** is always good to keep in mind: while low-brow, it can come in surprisingly handy.
   - Second, **descent**—i.e., using a given solution to derive the existence of a solution that is "smaller" in some well-defined way—is a common approach to medium and harder problems. When descent is possible from every solution, this approach proves unsatisfiability of the Diophantine equation and is known as *infinite descent*. Sometimes, however, the descent breaks down for small enough solutions; in these cases, all that remains is to enumerate the small solutions by brute force and then reverse the descent process to reconstruct all solutions (usually an infinite family).
   - Third, it is worth knowing at least the basic theory of **Pell's equation** $x^2 - dy^2 = 1$ (where d is nonsquare: in the square case, clearly no nontrivial solutions exist). The most important fact to commit to memory is that this equation always has an infinite family of solutions. It is also good to know that this family is generated by a *fundamental solution* (p, q) via "exponentiation," in the sense that $(p + q\sqrt{d})(p - q\sqrt{d}) = 1$ implies that $(p + q\sqrt{d})^n(p - q\sqrt{d})^n = 1$ as well, and the n-th powers can be expanded to $x \pm y\sqrt{d}$ form. Finally, in the general case $x^2 - dy^2 = c$ for $c \neq 1$, solutions may or may not exist, but if they do exist there must be at least one infinite family (generated by multiplying a particular solution by powers of a fundamental solution to $x^2 - dy^2 = 1$ and expanding as above).

The Nails

1. [2001 TST 8] Find all pairs of nonnegative integers (m, n) such that

$$(m + n - 5)^2 = 9mn.$$

2. [2002 TST 6] Find in explicit form all ordered pairs of positive integers (m, n) such that $mn - 1$ divides $m^2 + n^2$.

3. [1990/23 (ROM, IMO 3)] Find all positive integers n having the property that $\frac{2^n+1}{n^2}$ is an integer.

4. [1991/17 (HKG)] Find all positive integer solutions x, y, z of the equation $3^x+4^y = 5^z$.

5. [1992/13 (NZL, IMO 1)] Find all integer triples (p, q, r) such that $1 < p < q < r$ and $(1-p)(1-q)(1-r)$ is a divisor of $(pqr-1)$.

6. [1994/N2 (AUS, IMO 4)] Determine all pairs (m, n) of positive integers such that $\frac{n^3+1}{mn-1}$ is an integer.

7. [1995/N1 (ROM)] Let k be a positive integer. Prove that there are infinitely many perfect squares of the form $n \cdot 2^k - 7$, where n is a positive integer.

8. [1995/N4 (BUL)] Find all positive integers x and y such that $x + y^2 + z^3 = xyz$, where z is the greatest common divisor of x and y.

9. [1996/N4 (BUL)] Find all positive integers a and b for which

$$\left[\frac{a^2}{b}\right] + \left[\frac{b^2}{a}\right] = \left[\frac{a^2+b^2}{ab}\right] + ab.$$

10. [1997/6 (IRE)]

    (a) Let n be a positive integer. Prove that there exist distinct positive integers x, y, z such that
    $$x^{n-1} + y^n = z^{n+1}.$$

    (b) Let a, b, c be positive integers such that a and b are relatively prime and c is relatively prime either to a or to b. Prove that there exist infinitely many triples (x, y, z) of distinct positive integers x, y, z such that
    $$x^a + y^b = z^c.$$

11. [1997/17 (CZE, IMO 5)] Find all pairs of integers $x, y \geq 1$ satisfying the equation $x^{y^2} = y^x$.

12. [1998/14 (GBR, IMO 4)] Determine all pairs (x, y) of positive integers such that $x^2y + x + y$ is divisible by $xy^2 + y + 7$.

13. [1998/18 (BUL)] Determine all positive integers n for which there exists an integer m such that $2^n - 1$ is a divisor of $m^2 + 9$.

14. [2000/N4 (BRA)] Determine all triples of positive integers (a, m, n) such that $a^m + 1$ divides $(a+1)^n$.

15. [2001/N2 (COL)] Consider the system

$$\begin{aligned} x+y &= z+u, \\ 2xy &= zu. \end{aligned}$$

Find the greatest value of the real constant m such that $m \leq x/y$ for every positive integer solution x, y, z, u of the system with $x \geq y$.

16. [2002/N4 (GER)] Is there a positive integer m such that the equation

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}=\frac{m}{a+b+c}$$

has infinitely many solutions in positive integers a, b, c?

17. [2002/N6 (ROM, IMO 3)] Find all pairs of positive integers $m, n \geq 3$ for which there exist infinitely many positive integers a such that

$$\frac{a^m+a-1}{a^n+a^2-1}$$

is itself an integer.

18. [2003/N3 (BUL, IMO 2)] Determine all pairs (a, b) of positive integers such that

$$\frac{a^2}{2ab^2-b^3+1}$$

is a positive integer.

The Screws?

1. [2000/N6 (ROM)] Show that the set of positive integers that cannot be represented as a sum of distinct perfect squares is finite.

2. [2002/N1 (UZB)] What is the smallest positive integer t such that there exist integers $x_1, x_2, \ldots, x_t$ with $x_1^3 + x_2^3 + \cdots + x_t^3 = 2002^{2002}$?