Winter Camp 2009
Number Theory Tips and Tricks

David Arthur
darthur@gmail.com

1 Introduction

This handout is about some of the key techniques for solving number theory problems, especially Diophantine equations (equations with integer variables). Some of this stuff is pretty advanced, so if you have trouble following something, it's okay. Don't be afraid to ask questions!

I'm going to assume you already know some of the basics of number theory, especially modular arithmetic. I am also not going to spend much time covering theorems. If you want theorems or more background, I suggest checking out Naoki Sato's handout:

http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf

And once again, don't be afraid to ask questions!

2 Reduce mod n

Most IMO-level students will be familiar with the idea that an equation (or system of equations) can sometimes be solved by first reducing mod n, and then showing it has no solutions mod n. Here is one such problem:

Example: (*IMO 1986, #1*) Let d be any positive integer not equal to 2, 5, or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

Solution: The quadratic residues mod 16 are $\{0, 1, 4, 9\}$. Therefore, $2d - 1$ can only be a perfect square if $d \in \{1, 5, 9, 13\} \pmod{16}$, and $5d - 1$ can only be a perfect square if $d \in \{1, 2, 10, 13\} \pmod{16}$, and $13d - 1$ can only be a perfect square if $d \in \{2, 5, 9, 10\} \pmod{16}$. There is no d that simultaneously satisfies all three conditions, and the result follows. □

If you have done a lot of number theory before, this may seem like a fairly standard problem to you, and you might wonder that it made it onto the IMO. And it is a standard problem... sort of. We need to show a set of equations: $2d-1 = x^2, 5d-1 = y^2, 13d-1 = z^2$ has no integer solutions. So we reduce the equations mod 16, and by checking every possible value for d, we confirm that in fact, there are no possible solutions. There is one tricky part though: why should we choose 16 in particular? Nothing smaller works.

The art for these problems is choosing the right n. Here are some tips:

- Make n a prime power. The Chinese Remainder Theorem guarantees that looking at any polynomial mod xy is no better than looking at it mod x and then looking at it mod y

(assuming x and y are relatively prime). If there are variables in the exponents, you might want to break this rule, but even then, prime powers are still usually the right choice.

- If there are perfect squares in the equations, try n a power of 2. The fewer quadratic residues there are mod n, the better off you will be. If n is a power of 2, the number of quadratic residues mod n is $\left\lceil \frac{n}{6} \right\rceil + 1$. If n is a power of $p \neq 2$, the number of quadratic residues mod n is $\left\lceil \frac{pn}{2(p+1)} \right\rceil \geq \left\lceil \frac{n}{3} \right\rceil$. So, as you can see, powers of 2 are basically twice as good as the other choices! In practice, 4, 8, and sometimes 16 are good numbers to try.

- If there are m^{th} powers in the equation, the key is to choose $n = p^k$ so that $g = \gcd(m, (p-1)p^{k-1})$ is as large as possible. This is because the number of m^{th} powers mod n is approximately $\frac{n}{g}$. Usually you want to choose p, k so that $m|(p-1)p^{k-1}$.

- Make sure there is something to gain from doing modular arithmetic in the first place! The technique is very useful for showing an equation has no solutions. But if it has even one solution, it will also have a solution mod n for all n. Even if you can show all solutions are 1 mod 1,000,000,000, that still leaves an infinite number of possibilities to check!

- If the sum of the digits of an integer $S(n)$ is involved, always consider mod 9, because $S(n) \equiv n \pmod 9$.

3 Check the size of things

Almost as important as modular arithmetic in number theory is the fact that distinct integers differ by at least 1. An obvious fact, but a useful one nonetheless!

Example: (*see APMO 1999, #4*[1]) Find all positive integers (a, b) such that $a^2 + 4b$ and $b^2 + 4a$ are both perfect squares.

Solution: Suppose (a, b) is a solution. Assume without loss of generality that $a \leq b$. Then $b^2 < b^2 + 4a \leq b^2 + 4b < (b+2)^2$. It follows that $b^2 + 4a = (b+1)^2$, which implies $a = \frac{2b+1}{4}$. However, this is impossible because $\frac{2b+1}{4}$ is not an integer. Therefore, there are no solutions. □

In general, you should just always keep in mind approximately how large the quantities you are working with are. Take a step back, and ask if these bounds are pretty restrictive. If they are, you should probably investigate them pretty carefully. Here are a couple things to keep in mind:

- If $a|b$, then $b = 0$ or $|a| \leq |b|$.

- For all x, we have $x - 1 < \lfloor x \rfloor \leq x$, and $x \leq \lceil x \rceil < x + 1$.

- If x is a known integer and y is an unknown integer with $y \approx x$, then there aren't very many possibilities for y!

- Remember the division algorithm! Given integers n, m, there are unique integers a, b with $0 \leq b < m$, so that $n = am + b$. Sometimes, you can make this substitution, deal with the am part trivially, and then use inequality techniques to deal with the b part.

[1]The real APMO problem asks you to look for negative solutions as well. The same approach works, but there are more cases that you have to consider.

4 Factor

For many an Olympiad problem, the key step is a clever factoring or rewriting of the equation. Here are some useful things you can say after writing an expression as $x \cdot y$ for integers x, y:

- If $x, y > 1$, then xy is composite.
- If $xy = 0$, then $x = 0$ or $y = 0$.
- If xy is a power of a prime p, then x and y are powers of p as well.
- If x, y are relatively prime, and xy is a perfect k^{th} power, then x and y are perfect k^{th} powers as well.
- If $xy = a^2 + b^2$ with $\gcd(a, b) = 1$, then $x, y \not\equiv 3 \pmod 4$. (See example below.)

Example: Prove that there are no integer solutions (x, y) to $y^2 = x^3 + 23$.

Solution: The solution is based on the fact that if a prime p is congruent to 3 (mod 4), then -1 is not a quadratic residue modulo p. Remember that you were asked to prove this very useful fact during the pre-camp problem set!

In the given equation, note that if y is odd, then $x^3 \equiv 1 - 23 \equiv 2 \pmod 4$, which is impossible. If y is even, then $x^3 \equiv -23 \equiv 1 \pmod 4$. This leaves only the possibility that y is even and $x \equiv 1 \pmod 4$.

Now, write the equation as $4\left(\left(\frac{y}{2}\right)^2 + 1\right) = (x + 3)(x^2 - 3x + 9)$, and note that $x^2 - 3x + 9 \equiv 3 \pmod 4$. Therefore, there exists a prime $p \equiv 3 \pmod 4$ that divides $x^2 - 3x + 9$. This prime must also divide $\left(\frac{y}{2}\right)^2 + 1$. However, this would imply that -1 is a quadratic residue modulo p, which is impossible. □

Factoring is used in many places. Here are some things to watch out for:

- Completing the square: $x^2 + ax = \left(x + \frac{a}{2}\right)^2 - \frac{a^2}{4}$. You can then look at quadratic residues, or you can use this as part of a larger factoring. This can also set up a Pell's equation[2] (e.g. $x^2 + x = 2y^2$).
- Difference and sums of nth powers:
  $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + xy^{n-2} + y^{n-1})$,
  $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \ldots - xy^{n-2} + y^{n-1})$ if n is odd.
- Sophie Germain's identity: $x^4 + 4y^4 = (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2)$.
- Polynomials evaluated at two different points: There are many problems that revolve around the identity $x - y | P(x) - P(y)$ for P a polynomial with integer coefficients.
- Diophantine equations with variables in the exponents (e.g. $3^x - 2^y = 1$). For these problems, you almost always want to use modular arithmetic to show a couple exponents have to be multiples of some integer n, and then factor the equation as a difference (or sum) of n^{th} powers.

[2] A Pell's equation is an equation of the form $x^2 - Dy^2 = 1$, where D is a constant non-square. Such an equation always has an infinite number of integer solutions. If (x_1, y_1) is the smallest solution with $x > 1$, then the full set of solutions is given by $(\pm x_n, \pm y_n)$ where x_n and y_n are defined by $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.

5 Use infinite descent

Suppose you want to show an equation has no positive integer solutions, or it has no positive integer solutions of a certain type. With infinite descent, you do a proof by contradiction. Let x be the smallest "bad" solution. Then show there is another bad solution x' with $0 < x' < x$, giving a contradiction.

Warning: This only works for positive integers. You cannot assume an equation has a smallest rational solution, a smallest real solution, or a smallest negative solution! If an equation involves positive and negative integers, you can still do infinite descent if you take x minimizing $|x|$, but do *not* forget the absolute value!

If you want to do infinite descent, the real question is: how do you find x'?

Example: 2009 stones are given, each with positive integer weight. If any one stone is removed, the remaining stones can be split into two heaps with the same total weight, each containing exactly 1004 stones. Prove that all the stones weigh the same.

Solution: Let $\{w_i\}$ denote the weight of the stones, and let $W = \sum_{i=1}^{2009} w_i$. Assume the claim is false, and consider a counterexample minimizing W. If w_i is removed, then the remaining stones can be split into two equal-weight piles, so $W - w_i$ must be even. Since W is a constant, it follows that each w_i has the same parity.

If each w_i is even, then 2009 stones of weight $\{\frac{w_i}{2}\}$ is also a counterexample, but with smaller W. If each w_i is odd, then 2009 stones of weight $\{\frac{w_i+1}{2}\}$ is also a counterexample, but with smaller W (since, by assumption, we did not have every $w_i = 1$). Either way, we have a contradiction, and the result is proven. □

Here are some tips on how to set up infinite descent:

- If you can show every variable in an equation must be even (or a multiple of n), then you can often divide everything by n to get a smaller solution. *Example:* Solve $x^2 + y^2 = 3z^2$.
- Suppose you have an equation that is quadratic in one or more variables: e.g. $a^2+b^2 = abc+c$. Then if you know one root, you can find the other. For example, if $a = x$ is a root of the above equation, then $a = bc - x^2$ is another root. If the new value is smaller than the old one (but still positive), you can do infinite descent!

  This is an extremely important technique for the IMO, and it is called *root flipping* or *Vieta jumping*. Even outside of infinite descent solutions, you can still often learn something by looking at the other root of a quadratic.
- Sometimes it is easy to find larger solutions. You can then try to reverse the construction to get smaller solutions. *Example:* Call a positive integer "good" if it can be written in the form a^2+3b^2. Show that the product of two good numbers is good. Then reverse this construction to show that if $7n$ is good, then n is good.

6 Look at the order of elements mod n

You will often find yourself dealing with terms of the form x^y for various values y. To work with such expressions, it is helpful to remember the following:

Theorem 6.1. *Fix x and n with $\gcd(x, n) = 1$. There exists an integer m, called the order of x modulo n, such that $x^y \equiv 1 \pmod{n}$ if and only if $m|y$.*

In these terms, the very popular Fermat's little theorem states that if $x \not\equiv 0 \pmod{p}$, then the order of x mod p divides $p-1$.

Example: (*IMO Shortlist 2006, N5*) Find all integer solutions of the equation $\frac{x^7-1}{x-1} = y^5 - 1$.

Solution: This question is similar to $y^2 = x^3 + 23$, which was covered earlier.

Suppose $p \not\equiv 1 \pmod{7}$ is a prime divisor of $\frac{x^7-1}{x-1} = x^6+x^5+\ldots+1$, and let m denote the order of x modulo p. We know $x^7 \equiv 1 \pmod{p}$ so $m|7$. Also, by Fermat's little theorem, $m|p-1$. Since $p \not\equiv 1 \pmod{7}$, we know 7 and $p-1$ are relatively prime, so $m = 1$. Therefore, $x^1 \equiv 1 \pmod{p}$. Plugging this in, we have $0 \equiv x^6 + x^5 + \ldots + 1 \equiv 1 + 1 + \ldots + 1 \equiv 7 \pmod{p}$, and hence $p = 7$. It follows that if $z|\frac{x^7-1}{x-1}$, then z is congruent to 0 or 1 mod 7.

If $\frac{x^7-1}{x-1} = (y-1)(y^4+y^3+y^2+y+1)$, we therefore have $y \equiv 1, 2 \pmod{7} \implies y^4+y^3+y^2+y+1 \equiv 5, 3 \pmod{7}$. Either way, we have a contradiction. Therefore, the equation has no integer solutions. □

There are a couple generalizations of Fermat's little theorem that you should also know. First of all, what if p is not prime? To cover this case, we define $\phi(n)$ to be the number of positive integers less than n relatively prime to n. You can check that $\phi(p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}) = (p_1 - 1)p_1^{e_1-1} \cdot (p_2 - 1)p_2^{e_2-1} \cdot \ldots \cdot (p_k - 1)p_k^{e_k-1}$. Then:

Theorem 6.2. *(Euler's theorem) Fix x and n with $\gcd(x, n) = 1$. Then the order of x modulo n divides $\phi(n)$. Equivalently, $x^{\phi(n)} \equiv 1 \pmod{n}$.*

If n is a prime, then $\phi(n) = n - 1$, so this reduces exactly to Fermat's little theorem.

The next theorem is very powerful, and you should absolutely keep it in mind as the right intuition for how things work modulo prime powers. However, it is considered an advanced theorem, so quote it directly on contests at your own risk![3]

Theorem 6.3. *(Primitive roots) Suppose $n = p^k$ or $2p^k$ for some odd prime p and some positive integer k. Then, there exists x so that the order of x modulo n is exactly $\phi(n)$.*

Why is this so useful? It means that the set of integers relatively prime to n is precisely the set $\{1, x, x^2, \ldots, x^{\phi(n)-1}\}$ modulo n and the set of k^{th} powers relatively prime to n is precisely the set $\{1, x^k, x^{2k}, \ldots\}$. As an exercise, you might try using primitive roots to prove the following facts:

- If p is an odd prime, then -1 is a quadratic residue mod p^k if and only if $p \equiv 1 \pmod{4}$.
- Fix a prime p. Then p divides $1^k + 2^k + \ldots + p^k$ if and only if $p - 1$ does not divide k.

[3]On the IMO, if you use a known theorem and you have a correct solution, you will likely get your 7 points no matter what. The bad news is if you use a theorem or technique they don't like (e.g. coordinate geometry or Lagrange multipliers) and then make a mistake, you may not get much partial credit. Other Olympiads, including the CMO, are sometimes less generous even on correct solutions.

7 Problems

I have divided the problems into 3 types. The A problems are short (but not necessarily easy) problems that illustrate the concepts in these notes. The B problems are real Olympiad problems, most of which are quite challenging. The C problems are comparable to the hardest IMO number theory problems. If you can get them, you can get anything!

There are hints at the back, but only look at them after seriously trying the problems first.

A1. Let a, b, c, d be positive integers with $ab = cd$. Prove that $a + b + c + d$ is composite.

A2. Show that $4^n + n^4$ is composite for all integers $n \geq 2$.

A3. Prove that the system of equations:

$$x^2 + 6y^2 = z^2$$
$$6x^2 + y^2 = t^2$$

has no non-trivial integer solutions.

A4. Show that 19^{19} cannot be written as $m^4 + n^3$ for any integers m and n.

A5. Recall that e is given by the infinite sum $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$. Show that e is irrational.

B1. For which positive integers n do there exist positive integers a, b satisfying $a+b+n \cdot \gcd(a, b) = \text{lcm}(a, b)$?

B2. (*Korean Math Olympiad 1998, #1*) Find all pairwise relatively prime positive integers l, m, n such that

$$(l + m + n) \cdot \left(\frac{1}{l} + \frac{1}{m} + \frac{1}{n} \right)$$

is an integer.

B3. (*USAMO 2005, #2*) Prove that the system

$$\begin{aligned} x^6 + x^3 + x^3y + y &= 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 &= 157^{147} \end{aligned}$$

has no solutions in integers x, y, and z.

B4. (*Bulgarian Math Olympiad 1981, #4*) Prove that, if $1 + 2^n + 4^n$ is prime, then $n = 3^k$ for some integer k.

B5. (*IMO 1989, #5*) Prove that for each positive integer n, there exist n consecutive positive integers none of which is an integral power of a prime number.

B6. (*Russian Math Olympiad 1999, Grade 11, #5*) Four natural numbers have the property that the square of the sum of any two of the numbers is divisible by the product of the other two. Show that at least three of the four numbers are equal.

B7. (*IMO Shortlist 1996, N4*) Find all positive integers m and n such that $\left\lfloor \frac{m^2}{n} \right\rfloor + \left\lfloor \frac{n^2}{m} \right\rfloor = \left\lfloor \frac{m}{n} + \frac{n}{m} \right\rfloor + mn$.

B8. Prove that if $n \geq 3$, then $\lceil (3+\sqrt{5})^n \rceil$ is divisible by 8.

B9. (*IMO 2003, #2*) Determine all pairs of positive integers (a, b) such that

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

is a positive integer.

B10. (*Romania 1997*) Let $P(x), Q(x)$ be monic irreducible polynomials over the rational numbers. Suppose P and Q have respective roots α and β such that $\alpha + \beta$ is rational. Prove that the polynomial $P(x)^2 - Q(x)^2$ has a rational root.

B11. Prove that if n is a positive integer with the property that both $3n+1$ and $4n+1$ are perfect squares, then n is divisible by 7.

B12. (*IMO 1998, #3*) For any positive integer n, let $d(n)$ denote the number of positive divisors of n (including 1 and n itself).

Determine all positive integers k such that

$$\frac{d(n^2)}{d(n)} = k$$

for some n.

C1. (*IMO Shortlist 1998, N5*) Find all positive integers n for which there is an integer m with $2^n - 1 | m^2 + 9$.

C2. (a) (*IMO 2007, #5*) Let a and b be positive integers. Show that if $4ab-1$ divides $(4a^2-1)^2$, then $a = b$.

(b) (*IMO 1988, #6*) Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that

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

is the square of an integer.

C3. (*IMO Shortlist 2005, N6*) Let a and b be positive integers such that $a^n + n$ divides $b^n + n$ for every positive integer n. Show that $a = b$.

C4. (*IMO 1987, #6*) Let n be an integer greater than or equal to 2. Prove that if $k^2 + k + n$ is prime for all integers k such that $0 \leq k \leq \sqrt{n/3}$, then $k^2 + k + n$ is prime for all integers k such that $0 \leq k \leq n - 2$.

C5. (*IMO 1990, #6*) Prove that there exists a convex 1990-gon with the following two properties: (a) all angles are equal; (b) the lengths of the 1990 sides are the numbers $1^2, 2^2, 3^2, \ldots, 1990^2$ in some order.

C6. (*IMO Shortlist 2001, N6*) Is it possible to find 100 positive integers not exceeding 25,000, such that all pairwise sums of them are different?

C7. (*Chinese Math Olympiad 2006, #3*) Positive integers k, m, n satisfy $mn = k^2 + k + 3$. Prove there exist odd integers x, y so that either $x^2 + 11y^2 = 4m$ or $x^2 + 11y^2 = 4n$.

8 Selected Hints

A1. Substitute $d = \frac{ab}{c}$.

A2. Use Sophie Germain's identity.

A3. Add the equations, and do infinite descent.

A4. You want to reduce mod x. Remember the tips for choosing x.

A5. Assume that $e = \frac{m}{n}$ and multiply through by $n!$.

B1. Let $p = \gcd(a, b), q = \frac{a}{p}, r = \frac{b}{p}$.

B2. Show $m|n + l$. If $m \geq n, l$, that is pretty restrictive.

B3. Add the equations, and factor.

B4. Work out some examples. You should be able to see what must divide what.

B5. Use the Chinese Remainder Theorem.

B6. If p divides one of the numbers, what can you say about p?

B7. This is basically an inequality problem. If $m \geq n$, first show $m^2 > n$.

B8. Show $\left\lceil (3 + \sqrt{5})^n \right\rceil = (3 + \sqrt{5})^n + (3 - \sqrt{5})^n$.

B9. By root-flipping on $a^2 = 2ab^2x - b^3x + x$, it suffices to focus on the case $a \leq b$.

B10. Prove $Q(x) = \pm P(\alpha + \beta - x)$.

B11. Surprisingly, reducing mod 7^k doesn't work. But you can find *all* solutions using a Pell's equation. See the earlier footnote about them.

B12. Recall that if $n = \prod p_i^{e_i}$, then $d(n) = \prod(e_i + 1)$. Now try to do small values of k. Can you generalize your construction?

C1. You will need to show $2^{2^a} - 1$ has no prime divisors other than 3 that are 3 (mod 4).

C2. These problems both rely on infinite descent with root-flipping. For (a), first make the numerator of $\frac{(4a^2-1)^2}{4ab-1}$ more manageable. For (b), the tricky part is showing the new solution is positive.

C3. You don't need to consider every n. Choose one (depending on a, b) that is easy to work with.

C4. If x is a solution to $k^2 + k + n \equiv 0 \pmod{p}$, then so is $p - 1 - x$.

C5. Let ω_n denote a complex nth root of unity. Find an ordering $\ell_{i,j,k}$ of $\{1^2, 2^2, \ldots, 1990^2\}$ for which $\sum_{i=0}^{1} \sum_{j=0}^{4} \sum_{k=0}^{198} \omega_2^i \omega_5^j \omega_{199}^k \ell_{i,j,k} = 0$. (A simple ordering works – no need to be fancy.)

C6. The answer is yes, even for 101 numbers (hint, hint). Try setting it up so you can deduce $i + j$ and ij from $x_i + x_j$.

C7. Use infinite descent (but not root flipping for once) to prove that if $k^2 + 11 = 4mn$, then there exist a, b, c, d, not all even, satisfying $4m = a^2 + 11b^2$, $4n = c^2 + 11d^2$, $2k = ac + 11bd$.