Number theory: why things are true

James Rickards
jamesarickards@hotmail.com

1 Introduction

Number theory questions can be special in the sense that you can often get a good idea of "why" a problem must be true, and use this to point the way to a solution. Keeping this "why" in mind at all stages can prevent you from going down a fruitless path. It is also important to use the "olympiad metagame" by realizing that the given problem is solvable in a limited amount of time, so there has to be a reasonable solution (something that is no longer true when it comes to research). For certain problems, with this in mind, there is really only one viable possibility.

Rather than give an abstract list of possible "why's", let's go over some examples. Take some time to think about each problem, why it might be true, and how you may go about proving it.

2 Examples

Example 1 (APMO 1999 P4)**.** *Find all positive integers (a, b) such that $a^2 + 4b$ and $b^2 + 4a$ are both perfect squares.*

Example 2 (CMO 2003 P2)**.** *Call a positive integer n practical if every positive integer less than or equal to n can be written as the sum of distinct divisors of n (for example, 6 is practical). Prove that if x, y are practical, then so is xy.*

Example 3 (CMO 2004 P3)**.** *Let p be an odd prime. Prove that*

$$\sum_{k=1}^{p-1} k^{2p-1} \equiv \frac{p(p+1)}{2} \pmod{p^2}.$$

Example 4. *Show that 19^{19} cannot be written as $m^4 + n^3$ for any pair of integers (m, n).*

Example 5 (IMOSL 2005 N6)**.** *Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.*

Example 6 (IMO 1989 P5)**.** *Prove that for each positive integer k there exist k consecutive positive integers none of which is an integral power of a prime number.*

3 Solutions

Example 1

Why. *Since both a^2 and a^2+4b are squares, b has to be moderately large with respect to a. But since b^2 and b^2+4a are also squares, the opposite is true too!*

Solution. All that remains is to translate our "why" into formal statements. Since $a^2+4b > a^2$ and is equivalent to it modulo 2, we must have $a^2+4b \geq (a+2)^2 = a^2+4a+4$. Thus $b \geq a+1$. But by considering b^2+4a, we similarly get $a \geq b+1$, contradiction. Thus there are no solutions. □

Example 2

Why. *First, not every number is practical; for example odd numbers bigger than 1. In general, a practical number will have to have certain small divisors, and will have a large number of divisors. In that way, the problem statement seems believable.*
So how can we prove it? The only viable way would be to express all $n \leq xy$ as the sum of divisors of n.

Solution. Instead of trying to get n, let's first try to get close. Assume that $x \geq y$, and write $n = xq + r$ for some $0 \leq r < x$. Since $n \leq xy$, we must have $q \leq y$, whence $q = d_1 + \cdots + d_i$ for distinct divisors of y. But then we have $xq = xd_1 + xd_2 + \cdots + xd_i$, and $xd_1, \ldots, xd_i$ are all distinct divisors of xy! This puts us close, we just need to make up the remainder r. But $r < x$, so it's expressible as $r = e_1 + \cdots + e_j$, where $e_1, \ldots, e_j$ are distinct divisors of x. But then $e_k \leq r < x \leq xd_w$ for all k, w, so the entire set $\{e_1, \ldots, e_j, xd_1, \ldots, xd_i\}$ is a set of distinct divisors of xy which sum to $xq + r = n$, as desired. Thus xy is practical. □

Example 3

Why. *We can start with a sanity check: what about modulo p? Well, in that case $k^{2p-2} \equiv 1 \pmod p$, so*

$$\sum_{k=1}^{p-1} k^{2p-1} \equiv \sum_{k=1}^{p-1} k \equiv \frac{p^2+p}{2} \equiv 0 \pmod p,$$

as expected. Looking modulo p^2, we can't repeat this since the order of a typical element is p^2-p, much too different to $2p-1$. The only other reasonable thing would be to pair up terms in a convenient way, so that things cancel out. If we could somehow turn the p^2 into a p, then that would also be great!

Solution. The most natural pairing is k with $p-k$. Indeed, in this case we use the binomial theorem to get

$$k^{2p-1} + (p-k)^{2p-1} \equiv k^{2p-1} + (-k)^{2p-1} + (2p-1)p(-k)^{2p-2} \equiv p(2p-1)k^{2p-2} \pmod{p^2}.$$

Thus we can divide the whole thing through by p, and work modulo p instead! In particular, we get

$$\frac{1}{p}\sum_{k=1}^{p-1} k^{2p-1} \equiv \sum_{k=1}^{(p-1)/2} (2p-1)k^{2p-2} \equiv \frac{1-p}{2} \equiv \frac{1+p}{2} \pmod p,$$

where we can now use the fact that $k^{2p-2} \equiv 1 \pmod{p}$. Multiplying by p completes the solution! □

Example 4

Why. *There must be a sort of "barrier" preventing this number from being expressed, and the most natural such barrier would be looking mod p. What are good choices for p? We would want* $4, 3 \mid p-1$ *to cut down on residues, so* $p \equiv 1 \pmod{12}$.

Solution. Take $p = 13$, and note that the 4^{th} powers modulo 13 are $0, 1, 3, 9$, and the cubes modulo 13 are $0, 1, 5, 8, 12$. Adding these together, we hit all residue classes modulo 13 except 7 (mod 13). Conveniently, we also calculate that

$$19^{19} \equiv 6^{19} \equiv 6 * 36^9 \equiv 6 * (-3)^9 \equiv 6 * (-27)^3 \equiv -6 \equiv 7 \pmod{13},$$

completing the proof. □

Example 5

Why. *For all primes* $p \mid a^n + n$, *we must have* $p \mid b^n + n$, *which then implies that* $a^n \equiv b^n \pmod{p}$. *Assuming* $p \nmid a, b$, *this says that* $p \mid a^n + n$ *implies that* $(b/a)^n \equiv 1 \pmod{p}$. *This would pigeonhole n into certain equivalence classes modulo* $p-1$, *but* $p \mid a^n + n$ *should also incorporate information about* $n \pmod{p}$. *This should be enough to make a contradiction.*

Solution. To simplify things, fix any prime $p \nmid a, b$, and consider $n \equiv 1 \pmod{p-1}$. Then $a^n + n \equiv a + n \pmod{p}$, so let's also take $n \equiv -a \pmod{p}$. This is possible by the Chinese remainder theorem. Now we have $p \mid a^n + n \mid b^n + n$, whence $0 \equiv b^n - a^n \equiv b - a \pmod{p}$, and so $p \mid b - a$. But if $b \neq a$, then for large enough p this is a contradiction! Thus $a = b$. □

Example 6

Why. *The prime numbers are somewhat "sparse", so their powers should be as well. There are two viable approaches: one would be to construct k consecutive numbers with at least two prime factors, and the other would be a more analytic approach, where we show the existence without a construction.*

Solution. Take $2k$ distinct primes $p_1, \ldots, p_k, q_1, \ldots, q_k$, and by CRT find an integer n with $n \equiv -i \pmod{p_i q_i}$ for $i = 1, 2, \ldots, k$. Then $n+1, n+2, \ldots, n+k$ work. □

Solution. There is a constant C such that $\pi(n) := \{\text{primes} <= n\} \leq C\frac{n}{\log(n)}$. The number of prime power d^{th} powers less than n is at most the number of d^{th} powers less than n, which is at most $\sqrt[d]{n}$. We only need to consider $d \leq \frac{\log n}{\log 2}$, as for larger d, $x^d \geq 2^d > n$. In particular, the number of prime powers at most n is at most

$$C\frac{n}{\log(n)} + \sqrt[2]{n} + \sqrt[3]{n} + \cdots + \sqrt[\lfloor \log n / \log 2 \rfloor]{n} \leq C\frac{n}{\log(n)} + 2\log(n)\sqrt{n} \leq C'\frac{n}{\log(n)},$$

for some constant C'. Take n large enough so that $\frac{C'}{\log(n)} < \frac{1}{k}$, and WLOG assume that $k \mid n$. Then if every block $\{1, 2, \ldots, k\}, \{k+1, k+2, \ldots, 2k\}, \ldots, \{n-k+1, n-k+2, \ldots, n\}$ contained a prime power, then we would have at least $\frac{n}{k}$ such prime powers, contradiction. □

4 Problems

A-level problems should be short, but not necessarily easy. B and C level problems would be olympiad style and IMO level, with C being generally harder than B. This ordering is somewhat subjective, so don't be surprised if you find some problems to be out of place.

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

A2 If 5^n and 2^n both start with the same digit, what must that digit be? Can you find an example of this as well?

A3 Prove that the sequence $1, 11, 111, \ldots$ contains an infinite subsequence of relatively prime numbers.

A4 Prove that $a^2 + b^2 + c^2 = 2012$ has no solutions in positive integers.

A5 Let p be an odd prime. Prove that there exists an x such that $x^2 + 1$ is not a square modulo p.

A6 Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

B1 For $x \in (0, 1)$ let $y \in (0, 1)$ be the number whose n-th digit after the decimal point is the 2^n-th digit after the decimal point of x. Show that if x is rational then so is y.

B2 Prove that for every positive integer n there exists an n-digit number divisible by 5^n all of whose digits are odd.

B3 Prove that for each $n \geq 2$, there is a set S of n integers such that $(a-b)^2$ divides ab for every distinct $a, b \in S$.

B4 Prove that, if $1 + 2^n + 4^n$ is prime, then $n = 3^k$ for some integer k.

B5 b, m, n are natural numbers such that $b^n - 1$ and $b^m - 1$ have the same prime factors. Prove that $b - 1$ is a power of 2.

B6 Let a, b be odd positive integers. Define the sequence (f_n) by putting $f_1 = a$, $f_2 = b$, and by letting f_n for $n \geq 3$ be the greatest odd divisor of $f_{n-1} + f_{n-2}$. Show that f_n is constant for n sufficiently large and determine the eventual value as a function of a and b.

B7 Given an integer $n \geq 4$. $S = \{1, 2, \ldots, n\}$. A, B are two subsets of S such that for every pair of $(a, b), a \in A, b \in B, ab + 1$ is a perfect square. Prove that

$$\min\{|A|, |B|\} \leq \log_2 n.$$

B8 Find all natural numbers n greater than 2 such that there exist n natural numbers $a_1, a_2, \ldots, a_n$ such that they are not all equal, and the sequence $a_1a_2, a_2a_3, \ldots, a_na_1$ forms an arithmetic progression with nonzero common difference.

C1 Determine whether there exists an infinite sequence of nonzero digits $a_1, a_2, a_3, \cdots$ and a positive integer N such that for every integer $k > N$, the number $\overline{a_k a_{k-1} \cdots a_1}$ is a perfect square.

C2 Find all positive integers n such that there exists a unique integer a such that $0 \leq a < n!$ with the following property:

$$n! \mid a^n + 1$$

C3 Given a positive integer k, prove that there exists a positive integer N depending only on k such that for any integer $n \geq N$, $\binom{n}{k}$ has at least k different prime divisors.

C4 Let $n \geq 50$ be a natural number. Prove that n is expressible as sum of two natural numbers $n = x + y$, so that for every prime number p such that $p \mid x$ or $p \mid y$ we have $\sqrt{n} \geq p$. For example for $n = 94$ we have $x = 80, y = 14$.

C5 Let $k \in \mathbb{Z}^+$ and set $n = 2^k + 1$. Prove that n is a prime number if and only if the following holds: there is a permutation $a_1, \ldots, a_{n-1}$ of the numbers $1, 2, \ldots, n-1$ and a sequence of integers $g_1, \ldots, g_{n-1}$, such that n divides $g_i^{a_i} - a_{i+1}$ for every $i \in \{1, 2, \ldots, n-1\}$, where we set $a_n = a_1$.

C6 For all positive integers n, show that there exists a positive integer m such that n divides $2^m + m$.

C7 For every positive integer n with prime factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, define

$$\mho(n) = \sum_{i:\, p_i > 10^{100}} \alpha_i.$$

That is, $\mho(n)$ is the number of prime factors of n greater than 10^{100}, counted with multiplicity.

Find all strictly increasing functions $f : \mathbb{Z} \to \mathbb{Z}$ such that

$$\mho(f(a) - f(b)) \leq \mho(a - b) \quad \text{for all integers } a \text{ and } b \text{ with } a > b.$$

C8 Prove that for every prime $p > 100$ and every integer r, there exist two integers a and b such that p divides $a^2 + b^5 - r$.