Number Theory and the *abc* Conjecture

David Patrick
patrick@artofproblemsolving.com

November 10, 2012

Number Theory is the study of integers. Common topics include prime numbers, divisors and multiples, modular arithmetic, and Diophantine equations (equations in which we're looking for integer solutions).

Problems

1. A student at Harvard named Kevin
   Was counting his stones by 11
   He messed up n times
   And instead counted 9's
   And wound up at 2007

   How many different values of n could make this limerick true?

2. On the planet Remulak, the Coneheads play Funball. In Funball, a team scores 6 points for a slurf and 11 points for a gromstar. (A team starts with 0 points, of course.)
   (a) What is the maximum number of points that cannot be scored?
   (b) How many positive integers are unattainable scores? (You don't need to list them all; you just need to count them.)
   (c) Let a and b be positive integers such that all but 2009 positive integers are expressible in the form $ma + nb$, where m and n are nonnegative integers. If 1776 is one of the numbers that is not expressible, find $a + b$. (*From the USA Mathematical Talent Search*)

3. The **Euclidean Algorithm** is used to compute the greatest common divisor of two positive integers. The key step uses the fact that if $m \geq n$ are positive integers, then

   $$\gcd(m, n) = \gcd(m - n, n).$$

   The algorithm repeatedly applies the above step until the smaller number is 0, then uses the fact that $\gcd(n, 0) = n$. The "fast" version is to replace $\gcd(m, n)$ with $\gcd(n, r)$, where r is the remainder when dividing m by n.
   (a) Find an integer pair (x, y) that is a solution to the equation $35x + 22y = 1$.
   (b) Find a positive multiple of 31 that ends in the digits 174.
   (c) What is the smallest value of n such that there is some $m < n$ so that the fast version of Euclidean algorithm to compute $\gcd(m, n)$ takes at least 10 steps?

4. At a conference, n mathematicians sit around a circular table with n seats numbered $1, 2, 3, \ldots, n$ in clockwise order. They all get up to go on a coffee break, and then all sit back down again. One of the mathematicians notes that there is a positive number a such that:

   (i) for each k, the mathematician who was seated in seat k before the break is now seated in seat ka (where set $i + n$ is the same as seat i), and

   (ii) for every pair of mathematicians, the number of other mathematicians sitting between them (in either direction) after the break is different from the number of other mathematicians that had been sitting between them (in either direction) before the break.

   For what values of n is this possible? (*From the 2012 AIME contest*)

Number Theory and the *abc* Conjecture

David Patrick
patrick@artofproblemsolving.com

November 10, 2012

Wizards

Two wizards get on a bus.
First wizard: I have a positive number of children, each of which is a positive number of years old. The sum of their ages is the number of this bus and the product of their ages is my age.
Second wizard: Perhaps if you told me your age and the number of children, I could work out their individual ages.
First wizard: No, you could not.
Second wizard: Now I know your age.
What is the number of the bus? (Note: wizards can have any number of children and can be any positive integer years old.) *(From John Conway, via Paul Zeitz)*

The *abc* Conjecture

The *abc* conjecture (which is formally known as the Oesterlé-Masser conjecture) involves the really simple equation

$$a + b = c.$$

It turns out that it is relatively rare to have a solution to this equation such that no two of a,b,c have a common prime factor and where c is greater than the product of all the distinct primes that occur in a, b, and c. (Can you find an example of this?)

Now let's get technical. The conjecture says that for any $\epsilon > 0$ that we choose, there are only finitely many solutions to $a + b = c$ such that no two of a, b, c have a common prime factor and where

$$c > \text{rad}(abc)^{1+\epsilon},$$

where rad(abc) is the product of the prime factors of a, b, and c.
Question: what does this really mean?

The exciting news is that in August 2012, Shinichi Mochizuki of Kyoto University in Japan announced that he had a proof of the *abc* conjecture. It is about 500 pages long and has not yet been independently verified. If the proof is verified and the conjecture is true, it would prove a large number of previously unsolved problems in number theory.

Closing fun fact

What is the probability that two randomly chosen positive integers are relatively prime?

Number Theory and the *abc* Conjecture

David Patrick
patrick@artofproblemsolving.com

November 10, 2012

Solutions

1. We're trying to count the number of solutions in positive integers to $11m + 9n = 2007$. One "obvious" solution is $(m, n) = (0, 223)$. Then we note that we can get all other solutions by "trading" 11 n's for 9 m's. (One way to see that this is all possible solutions is that m must be a multiple of 9 because the other two terms are.) So $n = 223, 212, 201, \ldots$ all the way down to $(m, n) = (180, 3)$. There are $\boxed{21}$ solutions.

2. (a) One way to explore this problem is to make a chart:

$$\begin{array}{ccccccc} 0 & 11 & 22 & 33 & 44 & 55 & 66 \\ 1 & 12 & 23 & 34 & 45 & 56 & 67 \\ 2 & 13 & 24 & 35 & 46 & 57 & 68 \\ \vdots & & & & & & \\ 10 & 21 & 32 & 43 & 54 & 65 & 76 \end{array}$$

   In each row, we can make all the numbers starting with the smallest positive multiple of 6. Every row has a multiple of 6 that is 60 or less. We then see that $\boxed{49}$ is the smallest unattainable number.

   (b) More systematic is to prove the Chicken McNugget Theorem: if a and b are the point values, and $\gcd(a, b) = 1$, then every number that is at least $N = (a - 1)(b - 1)$ can be obtained, and if x and y are smaller than N such that $x + y = N - 1$, then exactly one of x or y can be obtained.

   > Proof: Let $a > b$. Then $\{0, b, 2b, \ldots, (a - 1)b\}$ span the residue classes mod a. Looking at a grid similar to the one above, we see that $(a - 1)b - a = ab - a - b$ is the largest number unattainable, so all numbers at least $ab - a - b + 1 = (a - 1)(b - 1)$ are attainable. For the second half of the theorem, x and y are in "opposite" residue classes mod a, so they mirror each other in the grid.

   In this particular problem, exactly half of $0, 1, \ldots, 49$ are unattainable, so there are $\boxed{25}$ unattainable scores.

   (c) All but 2009 positive integers being attainable tells us that $(a - 1)(b - 1) = 4018$, since half of the integers below 4018 are unattainable (and we must have $\gcd(a, b) = 1$, otherwise infinitely many integers would be unattainable). But $4018 = 2 \cdot 7^2 \cdot 41$, so the factorizations to consider are (assuming without loss of generality that $a > b$):

$$(a - 1, b - 1) = (1, 4018), (2, 2009), (7, 574), (14, 287), (41, 98), (49, 82),$$

   or

$$(a, b) = (2, 4019), (3, 2010), (8, 575), (15, 288), (42, 99), (50, 83).$$

   The first three give trivial ways to write 1776 (as a multiple of 2, 3, or 8). We can also rule out $(15, 288)$ and $(42, 99)$ because they're not relatively prime. So the answer must be $(50, 83)$, giving a sum of $\boxed{133}$. Indeed, $2241 = 27 \cdot 83$, so since $1776 + 2241 = 4017$ and 2241 is attainable, we know that 1776 is not attainable.

3. (a) We do the Euclidean algorithm:

$$\gcd(35, 22) = \gcd(13, 22) = \gcd(13, 9) = \gcd(4, 9) = \gcd(4, 5) = \gcd(4, 1) = 1.$$

We do the same steps with the equation:

$$\begin{aligned} 35 &= 22 + 13, \\ 22 &= 13 + 9, \\ 13 &= 9 + 4, \\ 9 &= 2 \cdot 4 + 1. \end{aligned}$$

Then we work backward:

$$\begin{aligned} 1 &= (1)9 + (-2)4 \\ &= (1)9 + (-2)(13 - 9) = (3)9 + (-2)13 \\ &= (3)(22 - 13) + (-2)13 = (3)22 + (-5)13 \\ &= (3)22 + (-5)(35 - 22) = (-5)35 + (8)22. \end{aligned}$$

(b) One way is to solve the equation $31n + 1000m = 1$, which will mean that $31n$ ends in the digits 001, and then multiply by 174. This is again a job for the Euclidean Algorithm:

$$\begin{aligned} 1000 &= (32)31 + 8, \\ 31 &= 3(8) + 7, \\ 8 &= 1(7) + 1, \end{aligned}$$

giving

$$\begin{aligned} 1 &= (1)8 + (-1)7 \\ &= (1)8 + (-1)(31 - 3(8)) \\ &= (-1)31 + (4)8 \\ &= (-1)31 + 4(1000 - (32)(31)) \\ &= (4)1000 + (-129)31. \end{aligned}$$

Uh-oh, that's negative. No problem: we can add 1000 to the coefficient of 31 as long as we subtract 31 from the coefficient of 1000. Thus $1 = (-27)(1000) + (871)(31)$. So $(871)(31)$ ends in 001, and hence $(174)(871)(31) = 4698174$ ends in 174.

(c) We can make a chart of the number of steps it takes to compute $\gcd(m, n)$ for $m \geq n$:

	1	2	3	4	5	6	7	8	9
1	1								
2	1	1							
3	1	2	1						
4	1	1	2	1					
5	1	2	3	2	1				
6	1	1	1	2	2	1			
7	1	2	2	3	3	2	1		
8	1	1	3	1	4	2	2	1	
9	1	2	1	2	3	2	3	2	1

The conjecture is that $\gcd(m, n)$ steps up at the Fibonacci numbers. This can be proved by an induction argument. Thus $\gcd(89, 144)$ is the smallest example that takes 10 steps.

4. Some experimentation might show that 5 is the smallest case that works. The requirement in (ii) for $n = 5$ just means that people sitting next to each other before must not be next to each other after,r and vice versa. This works using $a = 2$:

$$(1, 2, 3, 4, 5) \to (2, 4, 1, 3, 5)$$

We can also get it to work for $n = 7$.

Condition (i) holds if and only if a is relatively prime to n.

Condition (ii) means we must have

$$ak - aj \not\equiv \pm(k - j) \pmod{n}.$$

This means that $(a \pm 1)(k - j) \not\equiv (k - j) \pmod{n}$, so $a - 1$ and $a + 1$ must also be relatively prime to n.

Thus n works if and only if there exist three consecutive positive integers less than n that are all relatively prime to n. (Hence 5 works since $2, 3, 4$ fit the bill.) This rules out n even or n a multiple of 3. But all other n work with $a = 3$. So it works if and only if n is not a multiple of 2 or 3.

Wizards Solution

We know that given the number of children and the sum and product of the ages, the second wizard could not figure out the individual ages. Call a number n *unsolvable* if there are two sets of an equal number of numbers with sum n that also have the same product. In particular, the number of the bus is unsolvable. Note also that if n is unsolvable, then so is $n + 1$, because we can just add the number 1 to the two sets for n to get two sets for $n+1$ with the same sum and product. So once a number is unsolvable, all higher numbers are unsolvable too. 12 is unsolvable since $1 + 3 + 4 + 4 = 2 + 2 + 2 + 6$ and both sets have product 48. We can exhaustively check that every set of the same number of numbers that sum to 11 give a different product.

On the other hand, 13 is unsolvable with two different products: $1 + 6 + 6 = 2 + 2 + 9$ each have product 36, and $1 + 1 + 3 + 4 + 4 = 1 + 2 + 2 + 2 + 6$ each have product 48, and adding 1's to this means that every number greater than or equal to 13 is also unsolvable with at least two different products. By the second wizard's second statement, the bus number is not insolvable with multiple products, since he could figure out the product. Thus the bus number must be 12 (and the first wizard's age is 48, and he has 4 kids).

Closing fun fact answer

The two integers a and b must not both be multiples of p for all primes p. For any individual p, this occurs with probability $1 - \frac{1}{p^2}$, so the overall probability is

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Here $\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$.