Logical Hat problem, Puzzle Corner M/A 3, 2009, Joel Karnofsky, 7/28/2009

In the Logical Hat problem (Puzzle Corner M/A 3, 2009), two logicians, A and B, each wear a hat with a number on it. We are all told that they are error free reasoners and that A sees the sum and B sees the product of two integers, both ≥ 3. A says A1: "There is no way you can know the number on your hat." B says B1: "I now know my number." A says A2: "I now know my number. Both our numbers are less than 500." We are to find the numbers.

Let $S = x+y$ be the sum seen by A and $P = x \cdot y$ the product seen by B; about which they have made statements A1, B1 and A2. We will proceed by restricting the values for S that are consistent with error free reasoning by A and B until only one is left. We say the "possible products" are all products resulting from suitable x and y with sum S. For example, P is a possible product. Given a possible product, the "possible sums" are all sums resulting from suitable x and y with that product.

We are told both S and P are < 500 and clearly $S \geq 6$. Since the smallest possible product for S is 3(S-3) and 3(170-3) = 501, $S \geq 170$ would imply all possible products are > 500, so such S can be excluded.

A would error saying A1 if it is possible that B could immediately, essentially uniquely, factor P into suitable x and y. In particular, at least, (x,y) cannot be of the form (4,p), (2p,p) or (p,q), with p and q odd primes. We say a number is of type S1 if it can be written as p+4, 3p or p+q. We conclude S is not of type S1. Note that, at least, all small even numbers ≥ 6 can be written as p+q, hence are of type S1. Using the above, we can eliminate all but these 40 possibilities for S: 13, 19, 25, 29, 31, 37, 43, 49, 53, 55, 59, 61, 67, 73, 79, 81, 85, 89, 91, 95, 97, 99, 103, 109, 115, 119, 121, 125, 127, 133, 137, 139, 145, 147, 149, 151, 157, 163, 165, 169.

Notice that S is always one of the possible sums for any possible product. We say a possible product Q is of type P1 if all possible sums for Q other than S are of type S1. A key idea is: If Q is a possible product for S of type P1, then P = Q. The proof is as follows. It would not be an error for B to say B1 while looking at Q because it is true that there is only one possible sum for Q consistent with A1. Hence, it would be an error for A to be sure Q is not P. For A to say A2 without possibility of error, he must be sure all but one of the possible products are not P. Hence, any possible product he is unsure of must be P.

We use this idea in two ways. First, if there is a possible product of type P1 ≥ 500, then S can be excluded since solutions with $P \geq 500$ are excluded. Second, if there are two possible products of type P1, then A could not say A2, so S is again excluded.

Using the definitions, it is easy to check that the product is of type P1 in, at least, the three cases where (x,y) is of the form:

$(2^n,p)$

$(2p,q)$ with $2q+p = r+4$

$(2^n,p \cdot q)$ with $2^n p+q = r+4$ and $2^n q+p = s+4$

with p, q, r and s odd primes and $n \geq 2$.

Using these three cases and the "$\geq$ 500" test, (x,y) can be found to eliminate all S > 43 in the above list. As examples, showing the three cases:

$49 = 2^5+17 \quad 2^5\cdot17 = 544$

$127 = 2\cdot7+113 \quad 2\cdot113+7 = 229+4 \quad 2\cdot7\cdot113 = 1582$

$149 = 2^4+7\cdot19 \quad 2^4\cdot7+19 = 127+4 \quad 2^4\cdot19+7 = 307+4 \quad 2^4\cdot7\cdot19 = 2128$

and 7, 17, 19, 113, 127, 229 and 307 are all odd primes.

Using the first two cases above and the "two products" test, (x,y) can be found to eliminate all remaining possibilities for S other than 29 as follows:

$13 = 2\cdot3+7 = 2^3+5$

$19 = 2^3+11 = 2\cdot7+5$

$25 = 2\cdot3+19 = 2^3+17$

$31 = 2^3+23 = 2\cdot7+17$

$37 = 2\cdot3+31 = 2^3+29$

$43 = 2\cdot3+37 = 2\cdot7+29$

leaving the reader to check the ancillary conditions.

From $29 = 2^4+13$, the only possible solution is A wears $P = 2^4\cdot13 = 208$ and B wears S = 29. Because the statement of the problem implies there is a solution, this must be it.

Notice that no matter how hard we try to improve our logic while verifying this solution, we can never be sure that our logic is the same as, or as strong as, the logic that A and B use, so verification itself can never prove the result.

Appendix: It is interesting to see what happens if we are not told that S and P are < 500. Using a computer to find S's not of type S1 and with at most one possible product of type P1 gives the, probably infinite, sequence: 29, 89, 149, 179, 191, 209, 239, 251, … .

For all S's listed except 251, there is a single corresponding possible product of type P1, namely: 208, 1168, 2128, 2608, 8128, 3088 and 3568. By the arguments above, these (S,P) are all potential solutions. Maybe A and B could find better arguments than we have used to rule some out.

251 is a case for S where there are no possible products of type P1. This means the arguments above don't rule this case in or out. There are probably an infinite number of cases like this as well, starting: 251, 599, 701, 809, 959, 1019, 1211, 1271, 1589, … .

All the P's shown, in fact all found for S < 100,000, have the following properties: They are maximally divisible by an even power of 2 greater than 4 and all odd prime divisors are of the form 6k+1. It is not hard to see this implies all the S's are of the form 6k+5. This property for S continues to hold in those cases where there is no corresponding P. I don't know if these properties are true in general.