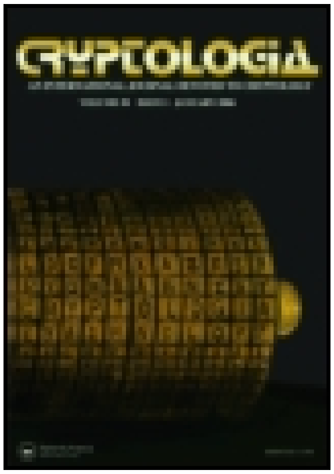

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

ON FACTORING JEVONS' NUMBER

Solomon W. Golomb [a]
[a] Communication Sciences Institute, Electrical Engineering Systems, University of Southern California, Los Angeles CA 90089-2565 USA.
Published online: 04 Jun 2010.

To cite this article: Solomon W. Golomb (1996) ON FACTORING JEVONS' NUMBER, Cryptologia, 20:3, 243-246, DOI: 10.1080/0161-119691884933

To link to this article: http://dx.doi.org/10.1080/0161-119691884933

ON FACTORING JEVONS' NUMBER

Solomon W. Golomb

ADDRESS: Communication Sciences Institute, Electrical Engineering Systems, University of Southern California, Los Angeles CA 90089-2565 USA.

ABSTRACT: In the 1870's, W.S. Jevons anticipated a key feature of the RSA algorithm for public key cryptography, namely that multiplication of integers is easy, but finding the prime factors of the product is hard. He presented a specific ten-digit number whose prime factorization, he believed, would forever remain unknown except to himself. In this paper, it is shown that Jevons' number could have been factored relatively easily, even in his own time.

KEYWORDS: Jevons, factorization, RSA algorithm.

In his book *The Principles of Science: A Treatise on Logic and Scientific Method*, written and published in the 1870's, William S. Jevons [1] observed that there are many situations where the "direct" operation is relatively easy, but the "inverse" operation is significantly more difficult. One example mentioned briefly is that enciphering (encryption) is easy while deciphering (decryption) is hard. In the same section of *Chapter 7: Induction* titled "Induction an Inverse Operation", much more attention is devoted to the principle that multiplication of integers is easy, but finding the (prime) factors of the product is much harder. Thus, Jevons anticipated a key feature of the RSA algorithm for public key cryptography [2], though he certainly did not invent the concept of public key cryptography. As an example of the multiplication vs factorization principle, Jevons wrote

> "Can the reader say what two numbers multiplied together will produce the number 8,616,460,799? I think it is unlikely that anyone but myself will ever know."

With a 10-place hand-held calculator, using only one memory location, and only the operations of subtraction, square, and square-root, it took me less than six minutes to factor Jevons' number J. My procedure was as follows:

Jevons wrote that the only method known (*to him*) for factoring a number N is to try dividing N by every prime up to $\sqrt{N}$. However, since J is odd and we are told that it has (at least) two factors, we can write $J = a^2 - b^2 = (a+b)(a-b)$.

We also strongly suspect, from Jevons' comments, that J is the product of only two primes, and that these are not too far apart in magnitude.

We set $a_0 = \lfloor\sqrt{J}\rfloor = 92824$, and let $a_k = a_0 + k$ for $k = 1, 2, 3, \ldots$. We look successively at $a_1^2 - J$, $a_2^2 - J$, $a_3^2 - J$, ... to see if any of these is a perfect square. [J is stored in memory, the a_k's are entered successively (using *my* memory), a_k is squared, J (from computer memory) is subtracted, the square-root button is hit, and unless we see an integer of only a few digits (which means $a_k^2 - J = b_k^2$, and we have $J = (a_k + b_k)(a_k - b_k)$), we proceed to a_{k+1}.] It was easy to do at least ten values of k per minute, with success at $k = 56$. Specifically, $a_{56} = 92880$, and $a_{56}^2 - J = (3199)^2 = b_{56}^2$. Thus $J = (a_{56} + b_{56})(a_{56} - b_{56})$. That is, 8,616,460,799 = 96,079 × 89,681.

This success led me to consider how easy or difficult it would have been for someone in the 1870's, using only hand calculation, to have succeeded in finding this factorization. I concluded that *at most* a few hours, and quite possibly less than an hour, would have been sufficient!

If we consider the equation $a_k^2 - J = b_k^2 \bmod 100$ (that is, we pay attention to only the last two digits of each number), since J ends in $\cdots 0799$, $-J \equiv +1(\mathrm{mod} 100)$, so a_k^2 and b_k^2 must end in *consecutive* two-digit numbers. The last two digits of n^2 are limited to values seen with n on the range of 0 to 25, and the only pairs of consecutive 2-digit endings are (00,01) and (24,25). Here, n^2 ends in **00** if and only if n ends in 0, while n^2 ends in **24** if and only if $n = 25 \pm 7(\mathrm{mod}\, 50)$. Thus, the only values of a_k which need be tried (to see if $a_k^2 - J$ is a perfect square) are those ending in 0, in 18, in 32, in 68, or in 82. Above $a_0 = \lfloor\sqrt{J}\rfloor = 92824$, we would need to look at only 92830, 92832, 92840, 92850, 92860, 92868, 92870, and 92880, with success on the eighth try (92880). However, even this is more hand computation than is actually necessary. Since $-J \equiv 201(\mathrm{mod} 1000)$ it is easily seen that when a_k ends in 0, the "tens digit" must be *even* in order for $a_k^2 - J \equiv b_k^2(\mathrm{mod} 1000)$ to be possible. (This eliminates 92830, 92850, and 92870 as candidates.) Also, when b_k^2 ends in 25, the digit *preceeding* "25" can only be 0, 2, or 6. But $92832^2 - J \equiv 224 + 201 \equiv 425(\mathrm{mod} 1000)$, so 92832 cannot be a solution for a. The only remaining candidates for a_k less than the "winning number" (92880) are now 92840, 92860, and 92868.

We can eliminate 92868 quite easily mod10^4 since $92868^2 - J \equiv 4625(\mathrm{mod}\ 10^4)$, but only numbers of the form $50n \pm 25$, n any positive integer, have squares ending in 625, and these end in either 0625 or 5625.

To test surviving values of a_k, such as 92840, 92860 and 92880, it is probably simplest, at this point, to calculate $a_k^2 - J$ by hand, and use the "square root algorithm" (which *was* taught in the schools in the 1870's) to see if this number is a perfect square. We find that $\sqrt{92840^2 - J} = \sqrt{2804801} = 1674.75^+$ and

$\sqrt{92860^2 - J} = \sqrt{6518801} = 2553.19^+$ *are not* integers, but $\sqrt{92880^2 - J} = \sqrt{10233601} = 3199$ *is* an integer. This method factors Jevons' number *quickly* because he picked the two prime factors of J relatively close together (they are in the approximate ratio of 15 to 14). There is a lesson in this for users of the RSA algorithm as well. The two primes p and q being used as factors of m should be sufficiently far apart that the attack $m = a^2 - b^2$ is as difficult computationally as other factorization methods which might be attempted. The theorem that every odd composite number m can be represented as $m = a^2 - b^2$, and that this can be used as a factorization technique, goes back to Fermat [3], [4] in 1643, and a refinement of Fermat's method involving continued fractions was used by D. N. Lehmer [5] in 1903 to factor Jevons' number. Lehmer wrote: "I think that the number has been resolved before, but I do not know by whom." The post-RSA rediscovery of Jevons' challenge and Lehmer's response appears to have been by József Dénes of Budapest, Hungary.

REFERENCES

1. Jevons, William S. 1958. *The Principles of Science: A Treatise on Logic and Scientific Method*, Macmillan & Co., London, 1873. Second edition (1877). New York: Dover Publications. Reprint.

2. Rivest, R., A. Shamir, and L. Adleman. 1978. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*. 21: 120-126.

3. Fermat, Pierre de. 1894. *Œuvres de Fermat*, tome 2, pp. 256-258. Paris: Gauthier-Villars et Fils.

4. Dickson, Leonard E. 1934. *History of the Theory of Numbers*. 1: Chapter XIV. New York, G. E. Stechert. p. 357.

5. Lehmer, D.N. 1907. "A Theorem in the Theory of Numbers." *Bull. Am. Math. Soc.*. 13: 501-502 (from a talk given in 1903 to the San Francisco section of the American Mathematical Society).

BIOGRAPHICAL SKETCH

Solomon W. Golomb received his BA from Johns Hopkins and his MA and PhD from Harvard, all in mathematics. After a year in Norway (1955-56) on a Fulbright fellowship, he joined the staff of the Jet Propulsion Laboratory, where he conducted and supervised research related to space communications. He has been on the faculty of USC since 1963, where he holds the title of University Professor, with appointments in Electrical Engineering, in Mathematics, and (as

Director of Technology) in the Annenberg Center for Communication. He is a member of the U. S. National Academy of Engineering, a Foreign Member of the Russian Academy of Natural Science, a Fellow of the IEEE and of the AAAS, and a Shannon Awardee of the Information Theory Society of the IEEE. He is the author of more than 200 technical papers, and of four books currently in print.