Pseudoprimes, Carmichael Numbers and an Ancient Chinese Fairy Tale, from Mike Mudge.

Revision note on congruence and modulus notation
Given three integers (whole numbers), A, B & C, we write A≡ B(C) (read A is congruent to B modulus C) if and only if A and B leave the same remainder when divided by C. It clearly follows that A — B is a multiple of C, *viz* A − B = kC for some integer k, either positive or negative. For example 273 ≡ 84(9) since 273 = 30×9 + 3, 84 = 9×9 + 3 and clearly 273 − 84 = 189 = 21×9.

The ancient Chinese are alleged to have considered possible solutions of $2^n \equiv 2(n)$ and further to have suspected that such n were prime. This 'fairy tale' is to be found in a paper by JH Jeans, in the *Messenger of Mathematics*, 27, 1897/8, dating the study of this congruence from the time of Confucius.

However, in his recent *Book of Prime Number Records*, Springer-Verlag 1988, Paulo Ribenboim destroys this myth firstly by observing that the Chinese mathematicians of the time had never formulated the concept of a prime number, and secondly by relating his own investigations of the literature revealing the source of an 'erroneous translation'.
Definition n is defined to be a **pseudoprime** to **base a** if: $a^{n-1} \equiv 1(n)$, and further n is not prime. Hence Ribenboim refers to the congruence $2^n \equiv 2$ (n) as the 'pseudo-Chinese congruence on pseudoprimes'!

In 1819 Pierre Sarrus found 341 = 11×31 as the smallest pseudoprime base 2. Pseudoprimes, to a given base, are quite rare. There are 882,206,716 primes less than 2×10^{10} but only 19,865 **pseudoprimes, base 2,** in the same range.

The sequence of pseudoprimes, base 2, commences: 341, 561, 645, 1005 . . . There are indeed even numbers satisfying $2^n \equiv 2(n)$, called **even pseudoprimes.** However, it should be noted that they are relatively rare, the smallest being 161038 = 2×73×1103 due to Lehmer 1950, the next being 215326. There are an infinity of even pseudoprimes, each must have at least two odd prime factors (Beeger 1951).

It is not known if there are infinitely many square pseudoprimes, the smallest examples are $1194649 = 1093^2$ and $12327121 = 3511^2$.
PROJECT A Determine the smallest pseudoprime to each of the bases 2, 3, 5 and 7. Hence, or otherwise, find the smallest pseudoprime for the simultaneous bases 2,3; 2,5; . . . then for 2,3,5; 2,3,7; . . . and finally for the quadruplet of bases 2,3,5,7.
Definition n is a Carmichael Number if:
$a^{n-1} \equiv 1(n)$ for *every* integer **a** satisfying $1 < a < n$ and such that a is relatively prime to n: that is, a and n have no common factors (divisors) other than unity, and further n is not prime.

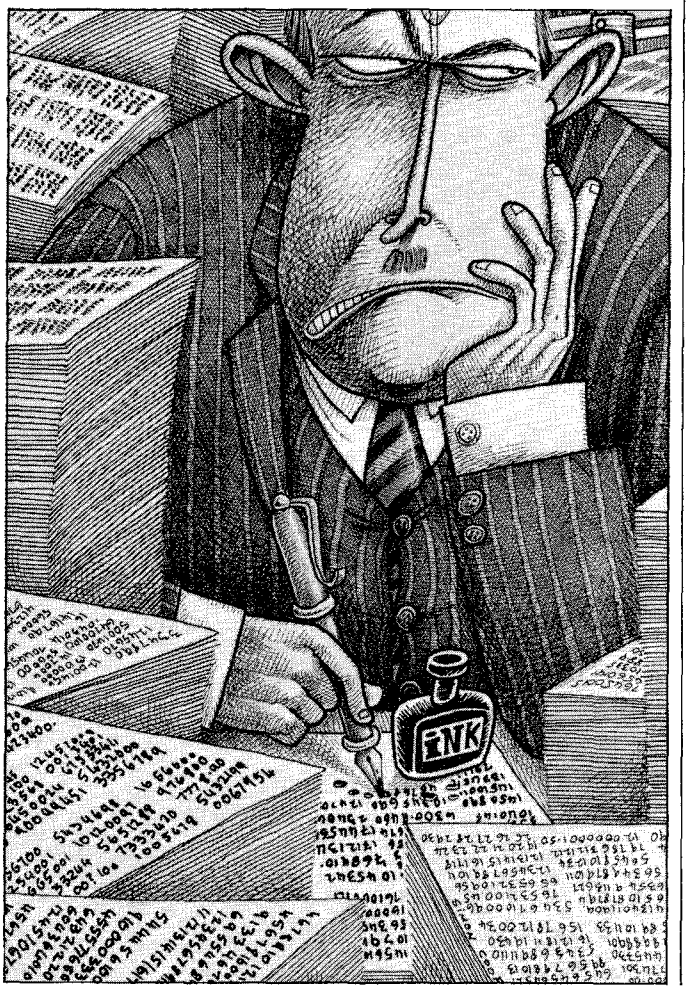
These numbers were first investigated by RD Carmichael in 1912 — he called them absolute pseudoprimes. (It should be noted that pseudoprimes are sometimes called Poulet Numbers after the investigations of P Poulet in 1926 and later in 1938).

It is not known if there exist infinitely many Carmichael Numbers. The sequence of such numbers commences: 561, 1105, 1729, 2465 . . .? The largest known Carmichael Number is believed to be that due to R Dubner in 1985 wit 1057 digits while in 1978 M Yorinaga found eight Carmichael Numbers each with 13 prime factors.
PROJECT B Construct and implement a computer algorithm to generate all Carmichael Numbers less than 3×10^5, say. Further consider the problem of verifying that a given number is indeed a Carmichael Number and hence verify the result of J Chernick, 1939, that if m≥1 and the three factors 6m + 1, 12m + 1 and 18m + 1 are all prime then their product is indeed a Carmichael Number.

Can this result be generalised to construct Carmichael Numbers having p prime factors?

Attempts at either or both of the above projects may be sent to Mike Mudge, 1 Dolboeth, Cwm Mabws, Llanrhystud, Dyfed SY23 5BB, tel (09746) 548, to arrive by 1 June 1990. Any communications received will be judged, using suitable subjective criteria, and a prize will be awarded by *PCW* to the st' contribution arriving by the closing date.

It would be appreciated if such submissions contained a brief description of the hardware used, details of programs and run times, and a summary of the results obtained; together with suggestions for further work in this area, all in a form suitable for publication in *PCW*. Please note that submissions can only be returned if a suitable stamped addressed envelope is provided.



Review, The Khinchin Constant
Khinchin's Constant, 2.6854520010653064 . . . is evaluated to some 68 decimal places in *MTAC*, vol 14, p371, 1960. Its continued fraction expansion, commencing 2;1,2,5,1,1,2,1,1,3,10,2 . . . is obtained in *MTAC*, vol 20, p446, 1966; while both quantities are available from Sloane NJ, *A Handbook of Integer Sequences*, Academic Press 1973, as entries 609 p73 and 47 p36 respectively.

The slow convergence, both of the infinite product and of the associated infinite series, proved to be a stumbling block for a number of contributors. Gareth Suggett using a BBC Micro and 323628 terms obtained K as approximately 2.6854(6) while Frank Webster using an Electron programmed in BBC Basic took 10^5 terms in 94 minutes and 10^6 terms in 14 hours to find K to 8 decimal places and its continued fraction to 13 partial quotients. A quasi-empirical argument by Frank led to 2.2 as a crude approximation to the limit described in Problem (3).

However, the very worthy prizewinner this month is Mathias Meuser of Annette, Kolb, Anger 15, 8000 Munich, West Germany for a combination of theoretical and computational investigations. The latter used interpretive Basic on a Tandy Model 100 with 24k of memory: obtained 10 decimal places eventually but three correct with 100 terms and two infinite integrals!

Readers interested in continued fractions are recommended to read A Ya Khinchin, *On Continued Fractions*, Dover paperback, together with the *MTAC* references given above.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions, either general or specific, for future Numbers Count articles.