For the "Comments" file of paper R25 of Volume 3 (1), 1996, 'Balanced Gray Codes', by Girish Bhat and Carla D. Savage

In the proof of Theorem 1 of the paper, three cases were considered, the third of which could occur only if $2^{n-1} \equiv -1 (\mathrm{mod}\ n)$ for some $n > 1$. The authors suspected that this case could never occur and this was verified by the following argument supplied by Kiran S. Kedlaya of Princeton University on November 13, 1996.

Claim: If $n > 1$ then 2^{n-1} is not congruent to $-1 (\mathrm{mod}\ n)$.
Proof. Assume you have such an n, and write $n - 1 = 2^k g$, where g is odd. For any prime p dividing n, we have 2^{n-1} congruent to -1 mod p. Let d be the smallest integer such that $p | (2^d + 1)$. Then $2^t \equiv -1 (\bmod p)$ implies t/d is an odd integer. (If we had a smallest counterexample t, then $|t - 2d|$ would also be a counterexample, yielding a contradiction.) In particular, $(n-1)/d$ is an odd integer h, so $d = 2^k j$, where $j = g/h$.

On the other hand, $2^{(p-1+d)} \equiv -1 (\mathrm{mod}\ p)$ by Fermat's little theorem, so $(p - 1 + d)/d$ is an odd integer, and $(p-1)/d$ is an even integer. Since $2^k | d$, we have $p \equiv 1 (\mathrm{mod}\ 2^{k+1})$. However, since this holds for all primes p dividing n, we conclude $n \equiv 1 (\bmod\ 2^{k+1})$, whereas $n - 1 = 2^k g$ is not divisible by 2^{k+1}, a contradiction.

Kiran Kedlaya
Princeton University
kkedlaya@math.princeton.edu

v3i1r16 — Comment by second author, Oct 22, 2005.

Frank Ruskey recently pointed out to us that an earlier construction and proof of the existence of balanced Gray codes for all n, attributed to T. Bakos, appears in the book *Truth functions and the problem of their realization by two-terminal graphs*, by A. Ádám, Akadémiai Kiadó, Budapest, 1968. This predates even the Robinson-Cohn paper. It also contains a proof of the question resolved by Kedlaya in the 1997 comment.

Carla Savage
North Carolina State University
savage@cayley.csc.ncsu.edu