CORRIGENDUM TO PSEUDOPRIMES AND FERMAT NUMBERS, #A23 OF VOLUME 24

Samuel S. Wagstaff, Jr.
Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, Indiana
ssw@cerias.purdue.edu

Posted: 8/3/26

1. The Mistake

The penultimate paragraph of Section 3 of the paper contains a misleading statement.

There we asked whether one could construct a weak pseudoprime base b for the Fermat number F_{12} which would factor F_{12} via (the proof of) Theorem 1 with one factor being the product of one or more of the six known prime factors. Then we suggested that if one multiplies b times an element s of the group $\mathbb{S}_{12}$ of Theorem 8, one might obtain another weak pseudoprime base that would split the large composite cofactor C1133.

The reason we thought this might succeed is that the product of two (weak or strong) pseudoprime bases is always a pseudoprime base and there are many more weak than strong bases (by Theorems 2 and 3), so if bs were a random base, it would have a good chance of being weak and, perhaps, of factoring C1133. Finally, there are $2^{14} = 16384$ elements s of $\mathbb{S}_{12}$ to try.

In fact, it is easy to perform the construction. Let P be any product of one or more of the six known prime factors. Let $Q = F_{12}/P$. Then $\gcd(P, Q) = 1$. Use the Chinese Remainder Theorem to solve the system

$$b \equiv 1 \pmod{P}$$
$$b \equiv -1 \pmod{Q}$$

modulo $PQ = F_{12}$. Then b is a weak pseudoprime base since $b^2 \equiv 1 \pmod{F_{12}}$ but $b \not\equiv \pm 1 \pmod{F_{12}}$. Also, using Theorem 1, we have $\gcd(b-1, F_{12}) = P$ and $\gcd(b+1, F_{12}) = Q$.

2. Why the Construction Is Never Useful

However, multiplication of b times a group element s never leads to anything new. If $s = 1$, the factorization is $P \times Q$. If $s = -1 \equiv 2^{4096} \pmod{F_{12}}$, the factorization

is $Q \times P$. Suppose $s \in \mathbb{S}_{12}$ and $s \not\equiv \pm 1 \pmod{F_{12}}$. Then modulo F_{12} we have $(bs)^2 \equiv b^2 s^2 \equiv s^2 \in \mathbb{S}_{12}$, which is a strong pseudoprime base by Theorem 8. Thus two group elements lead to a known factorization, while the other 16382 elements produce no factorization at all.

We tried other numbers for the right side of the Chinese Remainder Theorem problem. If at least one right side in the Chinese Remainder Theorem is not a group element, then one gets no factorization (unless one is extraordinarily lucky and guesses a weak pseudoprime base that gives a factorization). Note that 1 and $-1 \equiv 2^{4096} \pmod{F_{12}}$ are group elements. If one replaces 1 and -1 by any two group elements in the Chinese Remainder Theorem, one obtains only the known factorization $P \times Q$, perhaps for many group elements. For example, with P the least prime factor, and group elements 2 and 8 on the right side of the Chinese Remainder Theorem, one obtains the factorization $P \times Q$ 4096 times and no factorization 12288 times.

Here is why that happens. Let the right sides of the Chinese Remainder Theorem congruences be group elements 2^c and 2^d. Suppose first that $c = d$. Then $b = 2^c \in \mathbb{S}_{12}$ and for all $s \in \mathbb{S}_{12}$ we have $bs \in \mathbb{S}_{12}$ which is a strong pseudoprime base and gives no factorization.

Now suppose $c < d$. The other case $c > d$ is similar. Then the outcome (factorization or not) depends on whether s makes bs a weak or strong pseudoprime base. The only index at which F_{12} can be factored is the smallest m such that $(bs)^{2^m} \equiv 1 \pmod{F_{12}}$. If $(bs)^{2^{m-1}} \not\equiv -1 \pmod{F_{12}}$, then bs is a weak pseudoprime base and the factorization is $P \times Q$. If $(bs)^{2^{m-1}} \equiv -1 \pmod{F_{12}}$, then bs is a strong pseudoprime base and no factorization results.

The same arguments apply to all composite Fermat numbers with at least one known prime factor.

Acknowledgement. The author thanks Ryan Wallace for telling him that the construction in Section 1 is easy.