PROBLEM OF THE WEEK
Solution of Problem No. 1 (Spring 2004 Series)

**Problem:** Determine the positive integers $x < 10,000$ for which both $2^x \equiv 88 \pmod{167}$ and $2^x \equiv 70 \pmod{83}$. (You may use a calculator which is not programmable.)

**Solution** (by the Panel)

We need some general preliminaries:

For any integer $a > 1$ and any prime $p$ not dividing $a$, Fermat’s (“little”) theorem yields that the set of positive integer solutions $x$ of

$$a^x \equiv 1 \pmod{p}$$

is of the form \(\{x = kb : k = 1, 2, \ldots\}\) for some positive integer $b$ which divides $p - 1$. [See e.g. Hardy & Wright, An Introduction to the Theory of Numbers, 5th edition, OUP 1985, p.63, Theorem 71.]

Next, for any positive integer $c$ not divisible by $p$, consider the more general congruence

$$a^y \equiv c \pmod{p}.$$  

If $u$ and $v$ are positive integers with $u < v$ and if $y = u$ and $y = v$ both satisfy (2), then

$$c(a^v - a^u) \equiv c(a^v - a^u - 1) = a^v - a^u \equiv 0 \pmod{p},$$

whence (since $p$ does not divide $c$) in fact $a^v - a^u \equiv 1 \pmod{p}$, i.e. $x = v - u$ satisfies (1), so that $v - u = kb$ for some $k$. Hence, if $y = u$ is the smallest positive integer solution of (2), then the set of all positive integer solutions $y$ of (2) has the form

$$\{y = u + kb; k = 0, 1, 2, \ldots\}.$$ 

We now apply the generalities above to the case where $a = 2$ and $p, c$ are given either by $(p_1, c_1) = (167, 88)$ or by $(p_2, c_2) = (83, 70)$.

To calculate the corresponding $(b_j, u_j)(j = 1, 2)$ we first look at the positive divisors of $p_j - 1$. For $j = 1$, $p_1 - 1 = 166$ has only the divisors $1, 2, 83, 166$, of which clearly neither $x = 1$ nor $x = 2$ satisfies (1), but one verifies easily that $2^{83} \equiv 1 \pmod{167}$, and so $b_1 = 83$. To find the smallest solution $y = u_1$ of $2^y \equiv 88 \pmod{167}$, we test $y = 1, 2, \ldots$ in turn and find that $2^{12} \equiv 88$, i.e. $(b_1, u_1) = (83, 12)$. Similarly, $(b_2, u_2) = (82, 36)$.

It follows that any simultaneous solution $x$ of both $2^x \equiv 88 \pmod{167}$ and $2^x \equiv 70 \pmod{83}$ must be simultaneously of the forms $x = u_1 + k_1b_1$, $x = u_2 + k_2b_2$, so that

$$83k_1 - 82k_2 = u_2 - u_1 = 24,$$
whence \((k_1, k_2) = (34 + 82r, 24 + 83r)\) for some integer \(r\), which yields \(x = u_1 + k_1b_1 = 12 + 83k_1 = 2004 + 6806r\). For \(0 < x < 10,000\), we must take \(r = 0\) or \(1\), i.e. \(x = 2004\) or \(8810\).

Solved by:

**Undergraduates**: Paris Miles-Brenden (Jr. Phys/MA), Adam Welborn (So. CS)

**Graduates**: Vikram Buddh (MA), Jianguang Guo (Phys)

**Faculty**: Steven Landy (Phys, IUPUI)

**Others**: Prasenjeet Ghosh (New Delhi), Namig Mammadov (Baku, Azerbaijan), Troy Siemers (MA/CS, VMI, Lexington, VA), Christopher Smith (St. Cloud State, MN), Dhar-mashankar Subramanian (Chennai, India)

**Anonymous**: (by fax)

Two unacceptable solutions were received.