UIUC Department of Mathematics

PROBLEM OF THE WEEK
September 24, 2006

Universal primes

If a prime number is written out in decimal and then reinterpreted in a different basis, the resulting number need not be a prime. For example, 23 is a prime in the decimal system, but in base 11, it becomes $(23)_{11} = 25$, which is not a prime. On the other hand, since 61, $(61)_{11} = 67$, $(61)_{12} = 73$, and $(61)_{13} = 79$ are all primes, the number 61 is prime in base $b = 10$, and remains so in each of the bases $b = 11, 12, 13$ (though in the next basis, $b = 14$, it represents a composite number).

Call a prime number *universal*, if it remains prime with respect to *all* bases $b > 10$. Clearly, any single-digit prime is universal since it represents the same number in all such bases. Thus, the real question is:

> *Do there exist multi-digit universal primes? That is, do there exist digits* $a_1, a_2, \ldots, a_k \in \{0, 1, \ldots, 9\}$*, with* $k \geq 2$*,* $a_1 \neq 0$*, whose concatenation, interpreted as a base-b integer,* $(a_1 a_2 \ldots a_k)_b$*, is a prime for all bases* $b = 10, 11, 12, \ldots$*?*

—*Turn Page for Solution*—

Solution to "Universal primes"

Note that, given a string $a_1 a_2 \dots a_k$ with "digits" a_i, the integer represented by this string in base b is just the value of the polynomial $P(x) = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k$ at $x = b$. Further, multi-digit integers correspond to non-constant polynomials in this way. Thus, the question whether multi-digit "universal primes" exist reduces to the following question:

> *Are there non-constant polynomials $P(x)$ with nonnegative integer coefficients such that $P(x)$ is prime for all sufficiently large integers x?*

The answer to the latter question (and hence to the original question about the existence of multi-digit universal primes) turns out to be "no". This can be seen with a little bit of modular arithmetic as follows:

Let $n_0 = P(2)$ and note that, since $P(x)$ is non-constant (i.e., has degree at least 1) and has nonnegative integer coefficients, n_0 is an integer ≥ 2. Now consider any integer n with $n \equiv 2 \bmod n_0$. By the general properties of congruences, we have $n^i \equiv 2^i \bmod n_0$ for any nonnegative integer i, and hence $P(n) = a_1 n^{k-1} + a_2 n^{k-2} + \cdots + a_k n^0 \equiv a_1 2^{k-1} + a_2 2^{k-2} + \cdots + a_k 2^0 = P(2) \bmod n_0$. Since $P(2) = n_0$, it follows that $P(n) \equiv 0 \bmod n_0$, so $P(n)$ is divisible by n_0 for any such n. Moreover, since P has nonnegative coefficients and is non-constant, $P(x)$ is increasing in x and so $P(n) > P(2) = n_0$ for any $n > 2$. Thus, n_0 is a *proper* divisor of $P(n)$ for any integer $n > 2$ with $n \equiv 2 \bmod n_0$, and $P(n)$ is therefore composite for any such n, i.e., for $n = 2 + n_0, 2 + 2n_0, \dots$.