UIUC Department of Mathematics

PROBLEM OF THE WEEK
September 28, 2007

Determining a polynomial on the cheap

It is well-known that a polynomial of degree d is completely determined by its values at $d+1$ distinct points. Moreover, the number $d+1$ here is best-possible—knowing only d values is not sufficient to determine the polynomial. It may come as a surprise therefore that, if one restricts to polynomials with nonnegative integer coefficients, then the knowledge of only two cleverly chosen values, both at integers, is enough to uniquely determine the polynomial, regardless of its degree. This is the content of this week's POW:

Suppose $P(x)$ is an unknown polynomial, of unknown degree, with nonnegative integer coefficients. Your goal is to determine this polynomial. You have access to an oracle that, given an integer n, spits out $P(n)$, the value of the polynomial at n. However, the oracle charges a fee for each such computation, so you want to minimize the number of computations you ask the oracle to do. Show that it is possible to uniquely determine the polynomial after only two consultations of the oracle.

—Turn Page for Solution—

Solution to "Determining a polynomial on the cheap"

The solution is based on the following observation: If the coefficients of the polynomial are known to be bounded by a constant C, then for any integer $b > C$, these coefficients represent the digits in the base-b expansion of the number $P(b)$ and thus are uniquely determined by the number $P(b)$.

This argument requires only a single computation of a P-value, but it depends on having a bound C on the coefficients. However, since the coefficients of the polynomial are nonnegative, any value of the polynomial at a positive integer (and, in particular, $P(1)$) is necessarily an upper bound for its coefficients.

Thus, a suitable algorithm to determine $P(x)$ with two consultations of the oracle is:

1. Ask the oracle for the value $P(1)$.
2. Choose an integer $b > P(1)$ and ask the oracle for the value $P(b)$.
3. Expand $P(b)$ in base b; the base-b digits of this expansion are then the coefficients of $P(x)$.