MATHEMATICS PROBLEM 136

Show that the polynomial

$$p(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 4x^2 + 4x + 1$$

has no integer roots.

Each midshipman submitting a correct solution with a correct explanation to Problem 136 by 1700 Friday 20 February 2004 will be recognized as a solver on the next problem. Submit solutions to Prof. Wardlaw at mathprob@usna.edu (please no attachments!) or via his mailbox in Chauvenet 301.

Midshipman Stephen McMath submitted a correct solution to Mathematics Problem 135. A solution is on the back of this page and posted on the right wall at the Bancroft entrance to Chauvenet .

MATHEMATICS PROBLEM 135

The nth Fermat number is $F_n = (2^{(2^n)}) + 1$. Fermat knew that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ were prime, and he believed that all of these numbers were prime.

a. Show that if $h \circ k$ then $\gcd(F_h, F_k) = 1$.

b. Use part a to show that there are infinitely many primes.

c. (Extra credit) Find a nontrivial factor of F_5 .

Solution

a. Note that $F_1 - 2 = F_0$, $F_2 - 2 = F_0 F_1$, $F_3 - 2 = F_0 F_1 F_2$, and that $F_n - 2 = F_0 F_1 F_2 \ldots F_{n-1}$ implies that $F_{n+1} - 2 = F_n (F_n - 2) = F_0 F_1 F_2 \ldots F_{n-1} F_n$. It follows by induction that $F_k - 2 = F_0 F_1 F_2 \ldots F_{k-1}$ for all positive integers k. Thus if $h < k$ and $d = \gcd(F_h , F_k)$, then d divides both F_k and $F_k - 2$, so d divides 2. But d divides the odd number F_k , so $d = \gcd(F_h , F_k) = 1$.

b. For each positive integer k let p_k be the smallest prime divisor of F_k . Since there a is one F_k for each positive integer k, there is one prime p_k for each positive integer k, and by part a, no two of these are the same. Hence, there are infinitely many primes.

c. if p is a prime divisor of $F_5 = 2^{32} + 1$, then either p divides $2^k + 1$ for some k dividing 32, or 2^{32} ° -1 (mod p) but and $s = 64$ is the smallest exponent such that 2^s ° -1 (mod p). By Fermat's little theorem, 64 divides $p - 1$. Hence, $p = 64k + 1$ for some k. Trying $k = 1, 2, 3, \ldots$, we find that 641 divides $F_5 = 2^{32} + 1 = 4{,}294{,}967$, 297 = 641 ° 6,700,417. (Euler factored F_5 using an improvement of this method.)