189-346B/377B: Number Theory

Practice Midterm Exam

Monday, February 5, 2006

1. Using only basic properties of the gcd, (in particular, *without* using the fundamental theorem of arithmetic), show that, if an integer n divides the product ab and $\gcd(a, n) = 1$, then n divides b.

2. Find all the (positive and negative) integer solutions to the equation $y^2 - 2y = x^3$ in which y is odd.

3. Compute the value of the 11-th Fermat number $2^{2^{11}} + 1$ modulo 17. You should express your answer as an integer between 0 and 16.

4. Let φ be Euler's φ-function. Compute $\varphi(108)$. Show that there is no primitive root modulo 108.

5. Show that the polynomial $x^2 + 1$ has a root in $\mathbf{Q}_5$ and $\mathbf{Q}_{13}$ but not in $\mathbf{Q}_7$.