Math 4/5350

Last Homework

(Due Friday, May 1)

Problem. Let $N = 91$, $x = 2$, and $\epsilon = 1/2$.

(a) Find L, the smallest integer such that $N < 2^L$.

answer: $L = 7$

(b) Find $t = 2L + 1 + \lceil \log_2 (1 + 1/2\epsilon) \rceil$.

answer: $t = 16$

(c) Using your t from part (b), take the first t bits (starting from the left) of the following string and call it b: 01101010101010101010101010101010101010101

Then $b/2^t$ is the t-bit approximation of some as yet unknown fraction s/r where r is the order of $x \mod N$.

answer: $b = 0110101010101010$

(d) Write $b/2^t$ as a rational number (quotient of two integers).

answer: $27306/65536$

(e) Find the continued fraction expansion of the rational number $b/2^t$ from (d).

answer: [0, 2, 2, 2, 682, 4]

(f) Find the partial convergents of the continued fraction from part (e).

answer: [(0, 1), (1, 2), (2, 5), (5, 12), (3412, 8189), (13653, 32768)]

(g) Use the partial convergents from part (f) to find the fraction s/r mentioned in part (c).

answer: $s/r = 5/12$

(h) Use r from part (g), along with x, to factor N.

answer: $91 = 7 \cdot 13$