One-Way Functions

Tanya Khovanova

October 4, 2010

Class Discussion

One-way functions. Public Key Encryption. Calculation Time.

Warm Up

Exercise 1. 2008 HMNT. Find the sum of all positive integers n such that n divides $n^2 + n + 2$.

Exercise 2. 2008 HMNT. Johnny the grad student is typing all the integers from 1 to ∞, in order. The 2 on his computer is broken however, so he just skips any number with a 2. What's the 2008th number he types?

Exercise 3. 2008 HMNT. Find the number of distinct primes dividing $1 \cdot 2 \cdot 3 \cdots 9 \cdot 10$.

Cryptography

Exercise 4. Tanya's student Eli decided to make a more secure encoding. He added to his message the one-time pad key 13 times. Is this encryption more secure than just using a one-time pad? Why?

Exercise 5. The message contains 26 characters that are all different. The one-time key also has 26 all different letters. Prove that at least two characters in the enciphered text are the same.

Create a similar question about the Russian alphabet with 33 letters. What can you prove?

Exercise 6. Russian Cryptography Olympiad. It is known that the frequency of some letter in a message is between 10.5% and 11%. What is the smallest possible length of the message?

Competition Practice

Exercise 7. 2008 HMNT. Determine the last two digits of 17^{17}, written in base 10.

Exercise 8. 2008 HMNT. Call a number *overweight* if it has at least three positive integer divisors (including 1 and the number), and call a number *obese* if it has at least four positive integer divisors (including 1 and the number). How many positive integers between 1 and 200 are overweight, but not obese?

Exercise 9. 1959 Moscow Olympiad. Draw a circle that passes through two given points and cuts out a chord of a given length from a given circle.

Exercise 10. Fibonacci sequence is defined as: $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$. Prove that F_{5k} is divisible by 5.

Exercise 11. 2008 HMNT. Find the product of all real x for which $2^{3x+1} - 17 \cdot 2^{2x} + 2^{x+3} = 0$.

Exercise 12. 2008 HMNT. Find the sum of all primes p for which there exists a prime q such that $p^2 + pq + q^2$ is a square.