Problem 1. 50 points

Here are a couple of useful websites:

Use this one to check your hand calculation of the multiplicative modular inverse: e^{-1}: Link here.

Use this on to perform modular exponentiation. We are dealing with big numbers even for these toy examples and a regular calculator may give the wrong answer. Link here.

(a) Given the public key $e = 13, n = 77$ encrypt the message "HACKED" one letter at a time using ASCII to represent each letter. (Capitalization matters in ASCII)

(b) Decrypt the cyphertext you created in part (a) using the private key: $e^{-1} = 37$.

(c) Given primes p = 11 and q = 7, and $e = 13$ run through the RSA algorithm showing the encryption and decryption of the message "ACE" one letter at a time. Show the setup, encryption and decryption steps.

Solution

Problem 2. 50 points

Prove using mathematical induction the following claims:

(a) Let P(n) be the property "n¢ can be obtained using 2¢ and 5¢ coins". Use *weak mathematical induction* to prove that P(n) is true for all integers $n \geq 4$.

(b) Use *weak mathematical induction* to prove that $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

(c) Use *weak mathematical induction* to prove that $\forall n \geq 1, 3 \mid 2^{2n} - 1$.

(d) Use *strong mathematical induction* to prove that any integer greater than 1 is divisible by a prime number.

(e) Use *strong mathematical induction* to prove that $\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+, \exists q, r \ni n = d \cdot q + r \wedge 0 \leq r < d$. You will need to use the *Well-Ordering Principle* P. 620 of Rosen.

Solution