Discrete Structures

Worksheet 13

Spring 2022
February 15

---

1. Suppose $n = 101 \cdot 113$, $e_1 = 8765$, and $e_2 = 7653$. Note that 101 and 113 are primes.
   (a) One of e_1 and e_2 is a valid RSA encryption exponent (for modulus n) and the other is not. Explain which is which and why.
   (b) For the valid encryption exponent, compute d, the corresponding decryption exponent.

2. Consider the following defective cryptosystem: Let p be a large prime which is public. You encrypt a message m by computing $c = m^e \pmod{p}$ for some suitably chosen public encryption exponent e. How do you find a decryption exponent d such that $cd \equiv m \pmod{p}$?

3. Using induction, show that $(1+x)^n \geqslant 1 + nx$ for all $n \in \mathbf{N}$ and for all $x \in \mathbf{R}_{\geqslant -1}$.

4. *(Cummings, Proposition 4.4)* Using induction, show that the product of the first n odd natural numbers is equal to $\frac{(2n)!}{2^n n!}$.

---

6. Complete the following tasks for next lab (Friday). They will be presented at the beginning of the lab.
   (a) This question is about the RSA encryption scheme.
      i. Factor the number $n = 3844384501$ using the knowledge that $311776118522 \equiv 1 \pmod{3844384501}$.
      ii. Prove that the number 31803221 is not a prime number, using the fact that $2^{31803212} \equiv 27696377 \pmod{31803221}$.
   (b) *(Cummings, Theorem 4.16)* Using induction, show that if an undirected graph $G = (V, E)$ has $2n$ vertices and $n^2 + 1$ edges, then G contains a triangle.
   (c) Let $a_=1$, $a_2 = 8$, and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geqslant 3$. Use strong induction to prove that $a_n = 3 \cdot 2^{n-1} + 2 \cdot (-1)^n$ for all $n \in \mathbf{N}$.
   (d) Let $a_0 = 3$, $b_0 = 4$ and $c_0 = 5$. If

$$a_n = a_{n-1} + 2, \qquad b_n = 2a_{n-1} + b_{n-1} + 2, \qquad c_n = 2a_{n-1} + c_{n-1} + 2$$

   for all $n \in \mathbf{N}$, use strong induction to prove that $c_n - b_n$ is constant for all $n \in \mathbf{N}$.