CS 70 Spring 2013

Study Party Questions*

02/19/2013

1 Induct Me, Maybe?[1]

Prove that if n is a natural number and $1 + x > 0$, then $(1 + x)^n \geq 1 + nx$.

2 Some CS70 Stuff That I Used To Know

(a) Let m be a positive integer, and let a, b, and c be integers. Show that if $a \equiv b \pmod{m}$, then $a - c \equiv b - c \pmod{m}$.

(b) Consider the compound proposition $(\forall m \exists n [P(m, n)]) \rightarrow (\exists n \forall m [P(m, n)])$ where both m and n are integers. Determine the truth value of the proposition when $P(m, n)$ is the statement "$m < n$".

(c) Using a well-known theorem learned in class, compute $3^{302} \bmod 5$.

(d) Solve the following system of equations modulo 7 for x and y. Show your work.[2]

$$\begin{aligned} y &\equiv 5x - 3 \pmod{7} \\ y &\equiv 3x + 2 \pmod{7} \end{aligned}$$

(e) Give an RSA scheme based on primes $p = 7$ and $q = 5$, and describe a possible pair of public key (N, e) and a private key d. Use your public key to encrypt the message 6. What's the problem if you use $e = 3$ as part of your public key?

---

*Disclaimer: This review material does not provide a comprehensive coverage of the material that might be on the first midterm. All material covered in class, up to the end of Homework 4, are "fair game" for the test.

[1] http://vlsicad.ucsd.edu/courses/cse101-w13/handouts/Model_Solutions.pdf

[2] Spring 2005 Final Exam

3 As Long As You Love Me, I'll Keep Proposing, Don't Cross Me Off Yet, We Won't Be Rogue...[3]

(a) Consider the set of men $M = m_1, m_2, m_3$ with the following preferences on the set of women:

- $P_{m_1} = 1, 2, 3$
- $P_{m_2} = 1, 3, 2$
- $P_{m_3} = 3, 1, 2$

and the set of women $W = w_1, w_2, w_3$ with the following set of preferences on the set of men:

- $P_{w_1} = 3, 1, 2$
- $P_{w_2} = 3, 2, 1$
- $P_{w_3} = 2, 3, 1$

Run the traditional marriage algorithm on this example. How many times does the main loop run until reaching a stable matching in this case?

(b) Suppose the traditional marriage algorithm is run to produce a man-optimal stable pairing. Suppose then that one of the men moves one of the women to whom he never proposed up higher in his preference list (but all other preference lists remain unchanged). Then must the pairing remain stable?

(c) If man M does not propose to woman W in the traditional marriage algorithm, then can there be a stable pairing in which M is matched with W?

Good Luck with Your First CS70 Midterm!

[3] Fall 2010's Final Review Session