CS 70 Spring 2013

Study Party Solution*

02/19/2013

1 Induct Me, Maybe?[1]

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

Solution: We will prove the claim by induction on n.

- Base case: When $n = 0$ the claim holds since $(1 + x)^0 \geq 1 + 0x$.
- Inductive hypothesis: Now, assume as our inductive hypothesis that $(1+x)^n \geq 1 + nx$ for some value of $n > 0$.
- Inductive step: Now, we can show the following chain of inequalities:

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n(1+x) \\
&\geq (1+nx)(1+x) \quad \text{(by the inductive hypothesis)} \\
&\geq 1 + nx + x + nx^2 \\
&\geq 1 + (n+1)x + nx^2 \\
&\geq 1 + (n+1)x \quad (nx^2 \geq 0 \text{ since } n > 0)
\end{aligned}$$

$\therefore$ By induction, we have shown that $\forall n \in \mathbb{N}$, $(1 + x)^n \geq 1 + nx$.

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 $a - c \equiv b - c \pmod{m}$.

Solution: Since $a \equiv b \pmod{m}$ we have $m|(a-b)$. Hence there is an integer k such that $a - b = mk$. It follows that $(a - c) - (b - c) = a - b = mk$. This implies that $m|[(a - c) - (b - c)]$ so $a - c \equiv b - c \pmod{m}$.

*__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`

(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 "$m < n$".

Solution: This statement is **false**. Consider the left-hand side of the proposition. It is saying that "you pick any integer, and I can tell you something bigger." This part is true, because given any integer, I can always add 1 (or any positive integer) to it to find a bigger integer. Consider the right-hand side. This time, it is saying that "there exists an integer that is bigger than every integer." We know this statement is false because there is no such thing as a biggest integer. We also know that an implication of the form $T \rightarrow F$ is false, which is the answer to this question.

$\Rightarrow$ The order of the quantifiers is **very important**.

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

Solution: Based on *Fermat's Little Theorem*,

$$\begin{aligned} 3^4 &= 1 \,(\text{mod } 5) \\ 3^{300} &= (3^4)^{75} \\ &= 1^{75} = 1 \,(\text{mod } 5) \\ 3^{302} &= 3^2 \cdot 3^{300} \\ &= 9 \,(\text{mod } 5) = 4 \end{aligned}$$

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

$$\begin{aligned} y &\equiv 5x - 3 \,(\text{mod } 7) \\ y &\equiv 3x + 2 \,(\text{mod } 7) \end{aligned}$$

Solution: First solve for y. Multiply the first equation by 3 and the second equation by 5, giving

$$\begin{aligned} 3y &\equiv 15x - 9 \,(\text{mod } 7) \\ 5y &\equiv 15x + 10 \,(\text{mod } 7) \end{aligned}$$

Subtract the first equation from the second, giving $2y \equiv 19 \,(\text{mod } 7)$, or equivalently $2y \equiv 5 \,(\text{mod } 7)$. By applying the egcd algorithm, we see that $y = 6$ satisfies the constraint. Substituting into the first equation gives $6 \equiv 5x - 3 \,(\text{mod } 7)$, then $9 \equiv 5x \,(\text{mod } 7)$, and finally $2 \equiv 5x \,(\text{mod } 7)$. Again, $x = 6$ solves the congruence, hence the final answer are $x = 6$, $y = 6$.

(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. Use your public key to encrypt

[2] Spring 2005 Final Exam

the message 6. What's the problem if you use $e = 3$ as part of your public key?

Solution: Choosing $e = 5$ would be one solution, since 5 is relatively prime to $(p-1)(q-1) = 24$. The public key would then be $(N = pq, e)$ or $(35, 5)$. Using the egcd algorithm, you can also calculate that $d = e^{-1}$ mod 24, or $d = 5$, which is the private key. (This is a pretty bad encryption choice...)

In that case, 6^5 mod 35 can be computed using repeated squaring, and the encrypted message turns out to also be 6. The problem with $e = 3$ is that it's not relatively prime to 24, so $E(x)$ is not a bijection anymore.

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?

Solution: The algorithm takes 4 iterations to produce a matching.

Day	1	2	3	4
w_1	$\boldsymbol{m_1}, m_2$	$\boldsymbol{m_1}$	$m_1, \boldsymbol{m_3}$	$\boldsymbol{m_3}$
w_2				$\boldsymbol{m_1}$
w_3	$\boldsymbol{m_3}$	$\boldsymbol{m_2}, m_3$	$\boldsymbol{m_2}$	$\boldsymbol{m_2}$

(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?

[3] Fall 2010's Final Review Session

Solution: No. Counterexample: m_2 moves w_2 higher in the example above. In general, if M never proposes to W, then W may like M better than her current partner. If M then moves W higher than his current partner, the two of them can constitute a rogue pair.

(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?

Solution: Yes. TMA produces a male-optimal matching, and M only proposes to women he likes at least as much as his final partner. If there exists a stable pairing that is not male-optimal, then M would be paired with someone he does not propose to in TMA. This is of course possible in general.

Good Luck with Your First CS70 Midterm!