CS 135 Spring 2018: Quiz 2A Solutions.

NAME:

HONOR CODE STATEMENT:

Problem 1. (10 points) Point out the flaw in the following inductive argument (given that $x > 0$)
Claim: $\forall n \geq 0\ x^n = 1$.

Base case: $n = 0$. Since $x > 0$, it follows by definition that $x^0 = 1$.

(Strong) Inductive Hypothesis: For some $k \in \mathbb{N}$: $\forall i: 0 \leq i \leq k$: $x^i = 1$

Inductive Step: Note that $x^{k+1} = x^k . \frac{x^k}{x^{k-1}}$

From the strong inductive hypothesis $x^k = 1\ and\ x^{k-1} = 1$. Therefore, $x^{k+1} = 1 \cdot \frac{1}{1} = 1$, thereby establishing the inductive step.

The argument for the inductive step breaks down when $k = 0$: $x^{0+1} = x^0 \cdot \frac{x^0}{x^{-1}}$, but the inductive hypothesis does not apply to the denominator.

Problem 2. (15 points) Prove by induction the statement $\forall n \geq 5$: $2^n > n^2$.

a. State and establish the base case.

$$2^5 = 32 > 5^2 = 5^2$$

b. State the inductive hypothesis.

$P(k): 2^k > k^2, k \geq 5$

c. Establish the inductive step.

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &> 2 \cdot k^2, \text{(by the inductive hypothesis)} \end{aligned}$$

Now, since $k \geq 5$, it follows that $k^2 - 2k = k(k-2) > 1$, or $k^2 > 2k + 1$.

Thus, we have: $2^{k+1} > 2k^2 > k^2 + 2k + 1 = (k+1)^2$, thereby establishing the inductive step.

Problem 3. (10 points) Prove that if $a \equiv b \pmod{m}$ where $m \geq 2$ then $\gcd(a, m) = \gcd(b, m)$.
(Hint: To get started, let $a = mq_1 + r_1, b = mq_2 + r_2$.)

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Since $a \equiv b \pmod{m}$ we have that $m \mid (a - b)$. It follows that $m \mid r_1 - r_2$
Furthermore, since $-m < r_1 - r_2 < m$, it follows that $r_1 - r_2 = 0$, or $r_1 = r_2$.

By the GCD lemma, we have that $\gcd(a, m) = \gcd(m, r_1)$ and $\gcd(b, m) = \gcd(m, r_2)$. Since $r_1 = r_2$ it follows that $\gcd(a, m) = \gcd(b, m)$.

Problem 4. (15 points)

a. Find the inverse of 13 modulo 63. Show all steps of your calculation.

$$63 = 4 \cdot 13 + 11$$
$$13 = 11 + 2$$
$$11 = 5 \cdot 2 + 1$$

Therefore,

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 \\ &= 11 - 5 \cdot (13 - 11) \\ &= 6 \cdot 11 - 5 \cdot 13 \\ &= 6 \cdot (63 - 4 \cdot 13) - 5 \cdot 13 \\ &= 6 \cdot 63 - 29 \cdot 13 \end{aligned}$$

Thus, $13^{-1} \equiv -29 \equiv 34 \pmod{63}$

b. Solve the congruence $13x \equiv 5 \pmod{63}$.

Multiplying both sides by 13^{-1} gives us

$$\begin{aligned} x &\equiv 13^{-1} \cdot 5 \pmod{63} \\ &\equiv 34 \cdot 5 \pmod{63} \\ &\equiv 170 \pmod{63} \\ &\equiv 44 \pmod{63} \end{aligned}$$

CS 135 Spring 2018: Quiz 2B Solutions.

NAME:

HONOR CODE STATEMENT:

Problem 1. (10 points) Point out the flaw in the following inductive argument:
Claim: $\forall n \in \mathbb{N}: n^2 \leq n$.

Base Case: When $n = 0$, the statement $0^2 \leq 0$ is true.
Inductive Hypothesis: For some $k \in \mathbb{N}$: $k^2 \leq k$.
Inductive Step: Working backwards, we have that:

$$\begin{aligned} &(k+1)^2 \leq k+1 \\ \Rightarrow\ & k^2 + 2k + 1 \leq k+1 \\ \Rightarrow\ & k^2 + 2k \leq k \end{aligned}$$

Now, because $2k \geq 0$, it follows that

$$k^2 \leq k^2 + 2k \quad \Rightarrow \quad k^2 \leq k$$

By the inductive hypothesis, the last inequality is true. Therefore, the inductive step is established.

The inductive step calls for proving that $P(k) \Rightarrow P(k+1)$. The argument above instead shows that $P(k+1) \Rightarrow P(k)$. But this latter statement is true when its precedent is false. So besides establishing that $P(0)$ is true, nothing else has been proven true.

Problem 2. (15 points) Prove by induction the statement $\forall n \geq 0$: $1 + 2 + 2^2 + \cdots 2^n = 2^{n+1} - 1$

a. State and establish the base case.

$$P(0): 1 = 2^{0+1} - 1, \text{which is true as the RHS equals 1.}$$

b. State the inductive hypothesis.

$$P(k):\ 1 + \cdots + 2^k = 2^{k+1} - 1$$

c. Establish the inductive step.

$$\begin{aligned} 1 + \cdots + 2^{k+1} &= \left(1 + \cdots + 2^k\right) + 2^{k+1} \\ &= 2^{k+1} - 1 + 2^{k+1} \ \ \text{(using the inductive hypothesis)} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{(k+1)+1} - 1, \text{which establishes the inductive step.} \end{aligned}$$

Problem 3. (10 points) Prove that if $a \equiv b \pmod{m}$ where $m \geq 2$ then $\gcd(a, m) = \gcd(b, m)$. (Hint: To get started, let $a = mq_1 + r_1, b = mq_2 + r_2$.)

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Since $a \equiv b \pmod{m}$ we have that $m \mid (a - b)$. It follows that $m \mid r_1 - r_2$
Furthermore, since $-m < r_1 - r_2 < m$, it follows that $r_1 - r_2 = 0$, or $r_1 = r_2$.

By the GCD lemma, we have that $\gcd(a, m) = \gcd(m, r_1)$ and $\gcd(b, m) = \gcd(m, r_2)$. Since $r_1 = r_2$ it follows that $\gcd(a, m) = \gcd(b, m)$.

Problem 4. (15 points)

a. Find the inverse of 13 modulo 57. Show all steps of your calculation.

$$\begin{aligned} 57 &= 4 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2(13 - 2 \cdot 5) - 5 \\ &= 2 \cdot 13 - 5 \cdot 5 \\ &= 2 \cdot 13 - 5(57 - 4 \cdot 13) \\ &= 22 \cdot 13 - 5 \cdot 57 \end{aligned}$$

Thus, $13^{-1} \equiv 22 \ (mod\ 57)$

b. Solve the congruence $13x \equiv 5 \ (mod\ 57)$.

Multiplying both sides by 13^{-1} gives us:

$$\begin{aligned} x &\equiv 13^{-1} \cdot 5 \ (mod\ 57) \\ &\equiv 22 \cdot 5 \ (mod\ 57) \\ &\equiv 110 \ (mod\ 57) \\ &\equiv 53 \ (mod\ 57) \end{aligned}$$

CS 135 Spring 2018: Quiz 2C Solutions.

NAME:

HONOR CODE STATEMENT:

Problem 1. (10 points) Point out the flaw in the following inductive argument (given that $x > 0$)
Claim: $\forall n \geq 0 \;\; x^n = 1$.

Base case: $n = 0$. Since $x > 0$, it follows by definition that $x^0 = 1$.
(Strong) Inductive Hypothesis: For some $k \in \mathbb{N}$: $\forall i: 0 \leq i \leq k$: $x^i = 1$
Inductive Step: Note that $x^{k+1} = x^k . \frac{x^k}{x^{k-1}}$
From the strong inductive hypothesis $x^k = 1 \;\; and \; x^{k-1} = 1$. Therefore, $x^{k+1} = 1 \cdot \frac{1}{1} = 1$, thereby establishing the inductive step.

The argument for the inductive step breaks down when $k = 0$: $x^{0+1} = x^0 \cdot \frac{x^0}{x^{-1}}$, but the inductive hypothesis does not apply to the denominator.

Problem 2. (15 points) Prove by induction the statement $\forall n \geq 4$: $n! > 2^n$.
(Recall that $n! = n(n-1) \cdots 1$)

a. State and establish the base case.

$$P(4):\; 4! > 2^4$$

This is true because the LHS is 24 while the RHS is 16.

b. State the inductive hypothesis.

$$P(k):\; k! > 2^k, k \geq 4$$

c. Establish the inductive step.

$$\begin{aligned}(k+1)! &= (k+1)k! \\ &> 2 \cdot k! \;\; \text{since } k+1 > 2 \\ &> 2 \cdot 2^k \;\; \text{from the inductive hypothesis} \\ &= 2^{k+1} \;\; \text{thus establishing the inductive step}\end{aligned}$$

Problem 3. (10 points) Prove that if $a \equiv b \pmod m$ where $m \geq 2$ then $\gcd(a, m) = \gcd(b, m)$. (Hint: To get started, let $a = mq_1 + r_1, b = mq_2 + r_2$.)

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Since $a \equiv b \pmod m$ we have that $m \mid (a - b)$. It follows that $m \mid r_1 - r_2$
Furthermore, since $-m < r_1 - r_2 < m$, it follows that $r_1 - r_2 = 0$, or $r_1 = r_2$.

By the GCD lemma, we have that $\gcd(a, m) = \gcd(m, r_1)$ and $\gcd(b, m) = \gcd(m, r_2)$. Since $r_1 = r_2$ it follows that $\gcd(a, m) = \gcd(b, m)$.

Problem 4. (15 points)

a. Find the inverse of 11 modulo 63. Show all steps of your calculation.

$$\begin{aligned} 63 &= 5 \cdot 11 + 8 \\ 11 &= 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) \\ &= 3 \cdot 3 - 8 \\ &= 3(11 - 8) - 8 \\ &= 3 \cdot 11 - 4 \cdot 8 \\ &= 3 \cdot 11 - 4(63 - 5 \cdot 11) \\ &= 23 \cdot 11 - 4 \cdot 63 \end{aligned}$$

Therefore, $11^{-1} \equiv 23 \pmod{63}$

b. Solve the congruence $11x \equiv 5 \pmod{63}$.

Multiplying both sides by 11^{-1} we get:

$$\begin{aligned} x &\equiv 11^{-1} \cdot 5 \pmod{63} \\ &\equiv 23 \cdot 5 \pmod{63} \\ &\equiv 115 \pmod{63} \\ &\equiv 52 \pmod{63} \end{aligned}$$