CSE 321 Winter 2007 Midterm Solutions

1. (15 points)

   (a) Use the extended Euclidean algorithm to solve $33x \equiv 4 \pmod 7$ fox x.

   Solution: We will need to find an inverse of 33 modulo 7. We first use Euclid's algorithm to find the gcd of 33 and 7, then we will use the computation history of this algorithm to find the inverse. This process in full is the extended Euclidean algorithm.

   gcd(33,7) = gcd(7,5) = gcd(5,2) = gcd(2,1) = gcd(1,0) = 1.

   If we expand out the computations used in the execution of this algorithm, we will be able to find our inverse.

   (a) $33 = 4 \cdot 7 + 5$

   (b) $7 = 1 \cdot 5 + 2$

   (c) $5 = 2 \cdot 2 + 1$

   (d) $2 = 2 \cdot 1$

   To find an inverse of 33 modulo 7, we are looking for an s and t such that $1 = s \cdot 33 + t \cdot 7$. Such an inverse is guaranteed to exist, because 33 and 7 are relatively prime, as we showed above. We combine each of the three equations above to express 1 in this way.

   Equation (c) gives us $1 = 5 - 2 \cdot 2$.

   We then replace the second 2 above with larger terms, by using equation (b).

   $1 = 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$.

   Note that we could actually stop here if we recognized that $33 \equiv 5 \pmod 7$, so we could just find the inverse of 5 (mod 7). However, nobody did this.

   Finally, we replace 5 with larger terms by using equation (a). $1 = 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 = 3 \cdot 33 - 14 \cdot 7$.

   We now see that $1 = s \cdot 33 + t \cdot 7$, where $s = 3$, and $t = -14$. Rearranging this equation gives $1 + 14 \cdot 7 = 3 \cdot 33$. We can see that the left side is congruent to 1 mod 7, so 3 is the inverse of 33 modulo 7.

   Moving back to the linear congruence we were trying to solve, $33x \equiv 4 \pmod 7$. $3 \cdot 33 \equiv 1 \pmod 7$, so $3 \cdot 33x \equiv 3 \cdot 4 \pmod 7 \Leftrightarrow 1 \cdot x \equiv 12 \pmod 7 \Leftrightarrow x \equiv 5 \pmod 7$. Thus the linear congruence is solved.

(b) Find an inverse of 7 modulo 33.

Solution: The first important thing to notice is that this problem is not the same as the one above. It requires an inverse of 7 modulo 33, not an inverse of 33 modulo 7. Some people only attempted one of these problems, which seemed to indicate that they thought (a) and (b) were identical. That said, all the hard work for this problem has already been done in part (a). We know that the equation $1 = 3 \cdot 33 + (-14) \cdot 7$ holds. By rearranging this, we find that $1 + (-3) \cdot 33 = (-14) \cdot 7$. Clearly, -14 is an inverse of 7 modulo 33.

We accepted -14 with little to no explanation, if the work in part (a) was done. We also accepted any number congruent to -14 modulo 33, for example 19. Some people repeated the work of running and using the extended Euclid algorithm twice, which was fine. What wasn't acceptable was simply guessing numbers until one turned out to be an inverse.

2. (15 points) Let n be an integer. Prove that if nx is irrational, then x is irrational.

Solution: The simplest solution to this problem used proof by contraposition.

Proof: We prove that if x is rational, then nx is rational.

Assume that x is rational. Then there exist integers p and q s.t. $x = \frac{p}{q}$. Thus, $nx = n\frac{p}{q} = \frac{np}{q}$. n and p are integers, and the product of two integers is an integer, therefore, np is an integer. Since np and q are both integers, $nx = \frac{np}{q}$ is rational, by the definition of a rational number.

We have proved that if x is not irrational, it implies nx is not irrational, provided n is an integer. This is the contrapositive of the statement we wished to prove, and hence equivalent to our goal. This completes the proof.

Many people used a proof by contradiction, which is perfectly acceptable. There is a correspondence between proofs by contradiction and proofs by contraposition that works in many cases. Here, the proof assumes that nx is irrational but x is rational, then shows that x being rational implies that nx is rational, causing a contradiction.

Most people who tried to prove this theorem directly had some difficulty. If you simply start with the fact that $\neg\exists p\exists q\ nx = \frac{p}{q}$, it's harder to rigorously argue that when you divide nx by n there will still be no p and q s.t. $\frac{p}{q}$ equals it.

3. (15 points) Circle T or F to indicate whether each of the following statements is true or false. If the answer is false, *briefly* explain why. Assume positive integers for all numbers.

   (a) If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$. ..... F

   Let $a = 1, b = 2, c = 10, m = 10$, then it is true that $10 \equiv 20 \pmod{10}$, but $1 \not\equiv 2 \pmod{10}$.

   Some students tried to say that you cannot infer $m|(a-b)$ from $m|(ac-bc)$, but that does not mean you cannot prove it in some other fashion. A counterexample is sufficient to show that the implication does not hold.

   (b) If $a|c$, then $\exists b(a|b \wedge b|c)$. ..... T

   Let $b = c$ or $b = a$.

   (c) $\gcd(a, a \bmod b) \leq \gcd(a, b)$. ..... F

   If $a = 3, b = 5$, then gcd(3, 3 mod 5) = gcd(3, 3) = 3, whereas gcd(3, 5) = 1. Thus gcd(3, 3 mod 5) $\not\leq$ gcd(3, 5).

   (d) If $\gcd(a, b) = \gcd(b, c)$, then $\gcd(a, b) = \gcd(a, c)$. ..... F

   If $a = c = 10, b = 5$, then gcd(10, 5) = gcd(5, 10), but gcd(10, 5) $\neq$ gcd(10, 10).

   (e) $(\neg p \wedge \neg q) \rightarrow \neg(p \vee q)$ is a tautology. ..... T

   (f) $q \rightarrow (p \vee \neg p)$ is a tautology. ..... T

   (g) $(p \rightarrow q) \rightarrow (q \rightarrow p)$ is a tautology. ..... F

   If p is F and q is T, then $(p \rightarrow q)$ is T and $(q \rightarrow p)$ is F, which is F. Thus the original implication is not always T.

4. (15 points) Define the following predicates.

   - $M(x, y)$: "x is married to y"
   - $S(x, y)$: "x is a sibling of y"
   - $F(x)$: "x is female"
   - $P(x, y)$: "x is a (biological) parent of y"

   Let the universe for all variables be the set of all people. Do *not* use the uniqueness quantifier, $\exists!$. Express the following:

   (a) Everyone is married to at most one person.

   $$\forall x \forall y \forall z((M(x, y) \wedge M(x, z)) \rightarrow y = z)$$

   Some students wrote $\forall x \exists y M(x, y)$, but that translates to "Everyone is married to at *least* one person.

   (b) Tom is an only child (i.e. has no siblings).

   $$\forall x \neg S(x, \text{Tom}) \equiv \neg \exists x S(x, \text{Tom})$$

   (c) Siblings have a common (biological) parent.

   $$\forall x \forall y(S(x, y) \rightarrow \exists z(P(z, x) \wedge P(z, y)))$$

   (d) Alice is Bob's half-sister. (Alice and Bob have exactly one common biological parent.)

   $$F(\text{Alice}) \wedge \exists x(P(x, \text{Alice}) \wedge P(x, \text{Bob}) \wedge \forall y((x \neq y) \rightarrow (\neg P(y, Alice) \vee \neg P(y, Bob))))$$

   Many students who got close to this solution had the disjunction as a conjunction. This would mean that Alice and Bob have only one parent (the common parent). Alice and Bob presumably should each have another biological parent (that is not common to them).
   A common wrong answer was:

   $$\forall x \forall y((P(x, \text{Alice}) \wedge P(x, \text{Bob}) \wedge P(y, \text{Alice}) \wedge P(y, \text{Bob})) \rightarrow (x \neq y))$$

   This says that Alice and Bob cannot have more than one common parent, but it does not say that such a common parent actually exists.

5. (20 points) Prove that for every positive integer n, $\sum_{k=1}^{n} k2^k = (n-1)2^{n+1} + 2$.

Solution: As nearly everyone recognized, this theorem was intended to be proved using induction. Only mathematical induction was necessary, but there was nothing wrong with making the further assumptions of strong induction, even if you didn't use them.

Proof: Let $P(n)$ be the proposition: "$\sum_{k=1}^{n} k2^k = (n-1)2^{n+1} + 2$".

Base Case: We prove that $P(1)$ holds.

$$\sum_{k=1}^{1} k2^k = 1 \cdot 2^1 = 2 = (0)2^2 + 2 = (1-1)2^{1+1} + 2$$

Thus, $P(1)$ holds.

Inductive Hypothesis: Assume that $P(n)$ holds.

Inductive Step: We wish to prove that $P(n+1)$ holds, given the inductive hypothesis.

$$\begin{aligned}
\sum_{k=1}^{n+1} k2^k &= (\sum_{k=1}^{n} k2^k) + (n+1)2^{n+1} \\
&= (n-1)2^{n+1} + 2 + (n+1)2^{n+1} \\
&= (n-1+n+1)2^{n+1} + 2 \\
&= 2n2^{n+1} + 2 \;=\; n2^{n+2} + 2 = ((n+1)-1)2^{(n+1)+1} + 2
\end{aligned}$$

where the second equality holds from the inductive hypothesis.
This proves that $P(n+1)$ holds. Thus, by induction, $P(n)$ holds $\forall n \geq 1$.

Quite a few mistakes were made on this problem, which have also been common in induction on the homework. The most common mistake that people made was using a single expression $P(n)$ to represent both a mathematical function such as $\sum_{k=1}^{n}$ *and* a logical expression about that mathematical expression, such as "$\sum_{k=1}^{n} k2^k = (n-1)2^{n+1} + 2$". This is a significant mistake because it makes your proof very ambiguous. We've talked about this in section and in lecture, but still, only 2 points were taken off for this mistake, as long as it did not drastically obscure your proof.

Some people missed the summation, and thought that they were being asked to prove that $n2^n = (n-1)2^{n+1} + 2$. This proof is bound to break down somewhere along the line, as it did in different places for different people, because it simply isn't true.

Some people claimed to be doing induction, but then didn't use their inductive hypothesis at all, and attempted to show the equality by algebraic manipulation. This won't work out easily.

A few people formed their inductive hypothesis correctly by assuming that $P(n)$ holds, but then actually used the fact that $P(n+1)$ holds. This makes the proof trivial of course, (and incorrect) since this is what we are trying to show.

Finally, people often used the variables n and k interchangeably, after they had only defined one or the other. Points were rarely taken off for this, except when it made the proof particularly confusing. However, in general, it is important to be careful to pick variables for your induction, and use them consistently.

6. (10 points) What is $16^{15} \bmod 7$?

   There are many ways to solve this problem. One of the longer ways is to apply the modular exponentiation algorithm step-by-step:

   $15 = (1111)_2$, $x = 1$ and $power = 16 \bmod 7 = 2$.

   $i = 0 : a_0 = 1$: $x = 1 \cdot 2 \bmod 7 = 2$ and $power = 2^2 \bmod 7 = 4$.

   $i = 1 : a_1 = 1$: $x = 2 \cdot 4 \bmod 7 = 1$ and $power = 4^2 \bmod 7 = 16 \bmod 7 = 2$.

   $i = 2 : a_2 = 1$: $x = 1 \cdot 2 \bmod 7 = 2$ and $power = 2^2 \bmod 7 = 4$.

   $i = 3 : a_3 = 1$: $x = 2 \cdot 4 \bmod 7 = 1$ and $power = 2^2 \bmod 7 = 16 \bmod 7 = 2$.

   The final value of x is 1.

   Another way involved understanding exactly what the modular exponentiation algorithm is actually doing:

   We know that $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

   So $16^{15} \bmod 7 = 2^{15} \bmod 7$, because $16 \bmod 7 = 2$.

$$\begin{aligned} 2^{15} \bmod 7 &= (2^8)(2^4)(2^2)(2^1) \bmod 7 \\ &= ((2^8 \bmod 7)(2^4 \bmod 7)(2^2 \bmod 7)(2^1 \bmod 7)) \bmod 7 \\ &= ((256 \bmod 7)(16 \bmod 7)(4 \bmod 7)(2 \bmod 7)) \bmod 7 \\ &= (4 \cdot 2 \cdot 4 \cdot 2) \bmod 7 \\ &= 64 \bmod 7 \\ &= 1 \end{aligned}$$

   Yet another way of solving the problem:

   As above, we know we just need to solve $2^{15} \bmod 7$.

$$\begin{aligned} 2^{15} \bmod 7 &= (2^3)^5 \bmod 7 \\ &= 8^5 \bmod 7 \\ &= (8 \bmod 7)^5 \bmod 7 \\ &= 1^5 \bmod 7 \\ &= 1 \end{aligned}$$

7. (10 points) Find the flaw with the following "proof" that $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

   Basis Step: $a^0 = 1$ is true by the definition of a^0.

   Inductive Step: Assume that $a^j = 1$ for all nonnegative integers j with $j \leq k$. Then note that

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

   Try not to use more than 50 words.

   The "proof" fails when we try to compute a^1. This means that k is equal to 0 and we want to compute

$$a^{0+1} = \frac{a^0 \cdot a^0}{a^{0-1}}$$

   The denominator refers to a^{-1} which we don't know the value of, because by the inductive hypothesis, we only know a^j for all nonnegative $j \leq 0$—the only such j that applies is 0.

   Partial credit was given to those who recognized that there were not enough base cases, but did not explain why you needed more. Others recognized that there was a problem with a^1, but did not explain clearly how the "proof" broke down.

8. (1 BONUS point) Tell us something funny. If you're not particularly funny, then tell us something interesting. If you have nothing interesting to say either, then draw a picture of something. If nothing comes to mind, consider drawing Alex.

   Q: What did the shrimp say when he got caught in the seaweed?
   A: Kelp! Kelp!