CSE 20 - Winter 2008
Final Exam: 2008-03-18

Name: _____
Student ID number: _____

prob.	score
1	/6
2	/10
3	/8
4	/10
5	/16
6	/16
7	/10
8	/8
9	/8
10	/8
total	/100

Do not start until we announce the start. You will have 179 minutes. No books or calculators are allowed. One double-sided page of handwritten notes is allowed.

NOTE: If you need to make an assumption to solve a problem, or use a theorem from class, state the assumption or theorem.

1. (*6 points*) Circle the arguments that are valid.

1. All dogs have fleas.
   Snoopy is a dog.
   $\therefore$ Snoopy has fleas.

2. All beaches in San Diego are beautiful.
   Jones Beach is in New York City.
   $\therefore$ Jones Beach is not beautiful.

3. I did not learn anything in English class.
   $\therefore$ Everything I learned in English class is true.

Solution. The only valid arguments are 1, 3.

2. (*10 points*) Circle the statements that are true.

1. Every set that has a countable subset is countable.

2. Every student in this class (CSE 20, Winter 2008) who is younger than 5 years old, has maintained a perfect score.

3. There exists a computer program which, given as input any computer program X and any data set D, will correctly output the answer to whether program X, given input D, will halt or loop infinitely.

4. The following set is countable: $\{x \in \mathbb{Z} \mid 1 < x < 3\}$.

5. For all sets A and B, if $A \subseteq B$, then $A \cap B^c = \emptyset$.

Solution. The only true statements are 2, 4, 5.

3. (*8 points*) Prove that every integer $n \geq 2$ is either prime, or is a product of prime numbers. Do **not** use the Unique Factorization Theorem. (Hint: use induction).
Solution.
Proof:
Base case (n = 2): 2 is prime so the statement holds.

Inductive Hypothesis: Let $k \geq 2$ and assume the statement holds for all $2 \leq j \leq k$. That is j is either prime or is a product of primes.

Inductive Step: [w.t.s. $k+1$ is either prime or is a product of primes].
Since every integer greater than 1 is either prime or composite, we only need to consider those two cases:

1. Case $k+1$ is prime: then the statement holds, so we are done.
2. Case $k+1$ is composite: By definition of composite, then $k = m \cdot n$ where $m, n \in \mathbb{Z}$, and $1 < m \leq k$, $1 < n \leq k$. But that means the inductive hypothesis can be applied to both m and n. So m, n are each either prime or a product of primes. So their product, $k = m \cdot n$, is a product of primes. $\square$

4. (*10 points*)

a) Prove the following set equality, using the element method, or algebra involving other set equalities.

For all sets A and B, $A - (A \cap B) = A - B$.

Solution.
Proof:

$$\begin{aligned} A - (A \cap B) &= A \cap (A \cap B)^c \\ &= A \cap (A^c \cup B^c) \\ &= (A \cap A^c) \cup (A \cap B^c) \\ &= \emptyset \cup (A \cap B^c) \\ &= A \cap B^c \\ &= A - B \end{aligned}$$

b) Define $A = \{1, 2\}$, and $B = \{\emptyset, A, 3\}$. Write out the power set of B, $\mathscr{P}(B)$.

Solution.
First note that $B = \{\emptyset, \{1, 2\}, 3\}$. B has three elements, so its power set will have $2^3 = 8$ elements. The power set of B is:

$$\mathscr{P}(B) = \{\emptyset, \{\emptyset\}, \{\{1, 2\}\}, \{3\}, \{\emptyset, \{1, 2\}\}, \{\emptyset, 3\}, \{\{1, 2\}, 3\}, \{\emptyset, \{1, 2\}, 3\}\}$$

5. (*16 points*) Let $f : X \to Y$ and $g : Y \to Z$ be functions, and let $g \circ f : X \to Z$ be their composition. For each of the statements below, state whether it is true or false. If the statement is true, prove it.

a) If f is one-to-one and g is a bijection, then $g \circ f$ is a bijection.

b) If f is *not* one-to-one, then $g \circ f$ is *not* one-to-one.

c) If f is one-to-one, and $g \circ f$ is onto, then g is onto.

Solution.

a) If f is one-to-one and g is a bijection, then $g \circ f$ is a bijection. FALSE.

b) If f is *not* one-to-one, then $g \circ f$ is *not* one-to-one. TRUE.
Proof:
Let f and g be functions with domains and co-domains defined above. It would suffice to prove the contrapositive, that is, if $g \circ f$ is one-to-one, then f is one-to-one. So assume $g \circ f$ is one-to-one. So $\forall x_i, x_2 \in X$, if $(g \circ f)(x_1) = (g \circ f)(x_2)$, then $x_1 = x_2$. So, by definition of composition of functions, we have that $\forall x_i, x_2 \in X$, if $g(f(x_1)) = g(f(x_2))$, then $x_1 = x_2$. Assume for the sake of contradiction that f is not one-to-one. So there exists $x_3, x_4 \in X$ s.t. $f(x_3) = f(x_4)$ but $x_3 \neq x_4$. Since $f(x_3) = f(x_4)$, and since g is a function, $g(f(x_3)) = g(f(x_4))$, by definition of function. By definition of composition of functions, this means $(g \circ f)(x_3) = (g \circ f)(x_4)$. But since $x_3 \neq x_4$, this contradicts the fact that $g \circ f$ is one-to-one. $\square$

c) If f is one-to-one, and $g \circ f$ is onto, then g is onto. TRUE.
Proof:
Let f and g be functions with domains and co-domains defined above, and assume f is one-to-one, and $g \circ f$ is onto. In particular, $g \circ f$ is onto means $\forall z \in Z$, $\exists x \in X$ s.t. $(g \circ f)(x) = z = g(f(x))$. [w.t.s. g is onto, i.e. $\forall z \in Z$, $\exists y \in Y$ s.t. $g(y) = z$.]. Let $z \in Z$. Then since $g \circ f$ is onto, $\exists x \in X$, s.t. $g(f(x)) = z$. So let $y = f(x)$, which always exists and is an element of Y, since f is a function. $\square$

6. (*16 points*) Recall that the relation "congruence modulo 3" is defined as follows. $\forall x, y \in \mathbb{Z}$

$$x \; R \; y \;\Leftrightarrow\; x \equiv y \pmod 3 \;\Leftrightarrow\; 3 \mid (x - y)$$

a) Prove that R is an equivalence relation on $\mathbb{Z}$. (Do **not** use the theorem that congruence modulo n is an equivalence relation.)

b) List the distinct equivalence classes of R.

c) Prove that the distinct equivalence classes of R form a partition of $\mathbb{Z}$. To do so, you must prove both of the following statements:

(1) The union of the distinct equivalence classes is equal to $\mathbb{Z}$.

(2) The distinct equivalence classes are mutually disjoint.

Hint: use the definition of equivalence class, and the Quotient Remainder Theorem, in particular the existence, and uniqueness of the remainder, r. Also, for (1), remember to prove both directions of the subset relation to prove a set equality.

Solution.

a) **Proof:**
Reflexive: Let $x \in \mathbb{Z}$. Since $x - x = 0$, and $3|0$ because $0 = 0 \cdot 3$, we have that $3|x - x$, so $x \ R \ x$ by definition R.
Symmetric: Let $x, y \in \mathbb{Z}$, s.t. $x \ R \ y$. By definition of R, $3 \mid (x-y)$. By definition divisibility, $\exists k \in \mathbb{Z}$ s.t. $x - y = 3k$. So $y - x = -3k$. Since $-k \in \mathbb{Z}$, $3 \mid (y - x)$ by def. divisibility, so $y \ R \ x$ by def. R.
Transitive: Let $x, y, z \in \mathbb{Z}$, s.t. $x \ R \ y$ and $y \ R \ z$. [w.t.s. $x \ R \ z$.] By definition R, we have that $3 \mid (x-y)$ and $3 \mid (y-z)$. By def. of divis, $\exists k, \ell \in \mathbb{Z}$ s.t. $x - y = 3k$ and $y - z = 3\ell$. But $x - z = x - y + y - z = 3k + 3\ell = 3(k + \ell)$. Since $(k + \ell) \in \mathbb{Z}$, $3 \mid (x - z)$ by def. divisibility, so $x \ R \ z$ by def. R.

b) $[0], [1], [2]$

c) **Proof:**

(1) To show set equality, we will show the subset relation in both directions:
$[0] \cup [1] \cup [2] \subseteq \mathbb{Z}$:
By definition of equivalence class, that is $\forall a \in \mathbb{Z}$, $[a] \in \{x \in \mathbb{Z} \mid x \ R \ a\}$, every equivalence class is a subset of $\mathbb{Z}$. Since any element of a union of equivalences classes is a member of some equivalence class (by definition of union), and since every equivalence class is a subset of $\mathbb{Z}$, a union of equivalence classes is a subset of $\mathbb{Z}$.
$\mathbb{Z} \subseteq [0] \cup [1] \cup [2]$:
We must show that every integer is in one of the distinct equivalence class of R. By the QR theorem with $d = 3$, every integer can be written as either $3k$, $3k+1$, or $3k+2$ for some k in $\mathbb{Z}$. But these are exactly the set of distinct equivalence classes: for each $r \in \{0, 1, 2\}$, $[r] = \{x \in \mathbb{Z} \mid 3|x - r\} = \{x \in \mathbb{Z} \mid x - r = 3k, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x = 3k + r, k \in \mathbb{Z}\}$. Thus every integer is an some equivalence class of R.

(2) We must show that the distinct equivalence classes, $[0], [1], [2]$ are mutually disjoint. By the QR theorem with $d = 3$, for all $n \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. $n = dq + r$. This theorem also gives the uniqueness of r, and thus for each n and d, there is only *one* value of r for which the equality holds. Thus each $n \in \mathbb{Z}$ is in *exactly* one of the unique equivalence classes (and we gave the class for each integer in (1)). Since the equivalence classes are subsets of $\mathbb{Z}$, and since each element of $\mathbb{Z}$ is in only one of the distinct equivalence classes, each pair of distinct equivalence classes has an empty intersection. So by the definition of mutual disjointness, the set of distinct equivalence classes is mutually disjoint.

7. (*10 points*) Let $A = \{1, 2, 3, 4\}$. Let $R = \{(1, 1), (2, 3), (3, 2), (4, 1)\}$.

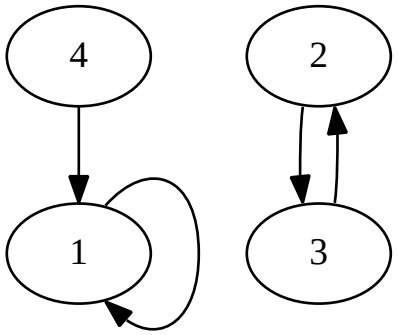
a) Draw the arrow diagram for the relation R defined on set A.

b) Circle the statements that are true.

1. R is reflexive.
2. R is symmetric.
3. R is transitive.
4. R is an equivalence relation.
5. R is a function from A to A.

6. R is a one-to-one function from A to A.
7. R is an onto function from A to A.
8. R is a bijection from A to A.

Solution.
a)



b) The only true statement is b5.

8. (*8 points*) Suppose A is a countable set, and B is an uncountable set. Circle the scenarios that are IMPOSSIBLE.

1. $A \subseteq B$
2. $B \subseteq A$
3. $|A| = |B|$
4. There exists a bijection $f : \mathbb{Z}^+ \to A$
5. There exists a bijection $g : \mathbb{Z}^+ \to B$
6. There exists an onto function $h : A \to B$
7. There exists a one-to-one function $c : A \to B$
8. There exists a bijection $d : B \to A$

Solution.
The following are the only impossible scenarios: 2, 3, 5, 6, 8.

9. (*8 points*) Let the sequence $a_1, a_2, a_3, \ldots$ be defined as follows:

$a_1 = 1$

$a_k = 2 \cdot a_{\lfloor k/2 \rfloor}$ for all integers $k \geq 2$.

Prove by induction that $a_n \leq n$ for all integers $n \geq 1$.
Solution.
Proof:

Base case (n = 1): $a_n = 1$ by definition of sequence and $1 \leq 1 = n$, as desired.

Inductive Hypothesis: Fix $j \geq 1$ and assume the claim is true for all $1 \leq i \leq j$, that is $a_i \leq i$.

Inductive Step: [w.t.s. $a_{j+1} \leq j + 1$]
By definition of the sequence, $a_{j+1} = 2 \cdot a_{\lfloor (j+1)/2 \rfloor}$.
But, by definition of floor, $\lfloor \frac{j+1}{2} \rfloor \leq \frac{j+1}{2} \leq j$, where the second equality holds for any $j \geq 1$. So we can apply the inductive hypothesis to $\lfloor \frac{j+1}{2} \rfloor$. By the inductive hypothesis, $a_{\lfloor (j+1)/2 \rfloor} \leq \lfloor \frac{j+1}{2} \rfloor$.
Applying this to the definition of the sequence yields:

$$a_{j+1} = 2 \cdot a_{\lfloor (j+1)/2 \rfloor} \leq 2 \cdot \lfloor \frac{j+1}{2} \rfloor \leq 2 \cdot \frac{j+1}{2} = j + 1$$

where we used the definition of floor for the second-to-last step. So $a_{j+1} \leq j+1$ as desired. □

10. (*8 points*)

a) Convert 10011_2 from binary (base 2) to decimal (base 10) notation.

b) Compute the greatest common divisor, *gcd*, of 42 and 12, using the Euclidean algorithm.

c) What is the smallest number of people such that, in any group of that size, at least three (3) people have the same first letter of their first name? Give a **proof** that your answer is correct.

Solution.

a) $10011_2 = 1 \times 2^4 + 1 \times 2^1 + 1 \times 2^0 = 16 + 2 + 1 = 19$.

b) $42 \mod 12 = 6$
$12 \mod 6 = 0$
Since 6 the divisor that yields a remainder of zero in the Euclidean algorithm, $gcd(42, 12) = 6$.

c) $2 \cdot 26 + 1 = 53$. Our claim is that in any group of 53 people, at least 3 people in the group share the same first initial.
Proof by contradiction:
Assume that there exists a group of 53 people such that no set of three people share the same first initial. In other words, for each letter in the alphabet, at most 2 people in the group have that letter as their first initial. But then, by the generalized pigeonhole principle (contrapositive form), the size of the group is at most $2 \cdot |\text{alphabet}| = 2 \cdot 26 = 52$. But this a contradiction because the size of the group is $53 > 52$.