Math 300.2 Midterm 2 review questions

Paul Hacking

April 4, 2012

Reading: Gilbert and Vanstone, Chapters 3,5,6.

(1) Show that if $x \in \mathbb{Z}$ then x^2 is congruent to 0, 1, or 4 modulo 8.

(2) Find all solutions of the following congruences.

  (a) $x^2 \equiv 3 \bmod 11$.
  (b) $x^3 \equiv 2 \bmod 5$.
  (c) $x^2 + 3x + 3 \equiv 0 \bmod 7$.

(3) Find all solutions of the following linear congruences or prove that no solutions exist.

  (a) $3x \equiv 8 \bmod 11$.
  (b) $12x \equiv 6 \bmod 18$.
  (c) $21x \equiv 5 \bmod 51$.

(4) Find all solutions of the following pairs of linear congruences or prove that none exist.

  (a) $x \equiv 1 \bmod 3$, $x \equiv 4 \bmod 7$
  (b) $x \equiv 8 \bmod 15$, $x \equiv 7 \bmod 33$.

(5) Find one solution of the congruence $x^2 \equiv 58 \bmod 77$. [Hint: Use the Chinese remainder theorem.]

(6) Give the definition of the Euler phi function $\phi\colon \mathbb{N} \to \mathbb{N}$.

(a) Show carefully that for p a prime number and $\alpha \in \mathbb{N}$ we have $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.

(b) State a general formula for $\phi(m)$ in terms of the prime factorization of m, and use it to compute $\phi(108)$.

(7) Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

(a) Show carefully that if $a \equiv c \bmod m$ and $b \equiv d \bmod m$ then $ab \equiv cd \bmod m$.

(b) Use part (a) and mathematical induction to prove that if $a \equiv b \bmod m$ then $a^n \equiv b^n \bmod m$ for each $n \in \mathbb{N}$.

(8) Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$

(a) Show that if $ab \equiv ac \bmod m$ and $\gcd(a, m) = 1$ then $b \equiv c \bmod m$.

(b) Show by example that the condition $\gcd(a, m) = 1$ is necessary in part (a).

(9) Let R be a relation on a set S. What does it mean to say that R is an equivalence relation? Which of the following relations are equivalence relations? Justify your answers carefully.

(a) $S = \mathbb{Z}$, $xRy \iff 7 \mid (x - y)$.

(b) $S = \mathbb{R}$, $xRy \iff x \le y$.

(c) $S = \mathbb{N}$, $xRy \iff x \mid y$.

(d) $S = \mathbb{R}^2$, $(a, b)R(c, d) \iff \sqrt{(a-c)^2 + (b-d)^2} \le 1$.

(e) $S = \mathbb{R}^2$, $(a, b)R(c, d) \iff \exists\lambda \in \mathbb{R}$ such that $\lambda > 0$ and $(a, b) = (\lambda c, \lambda d)$.

(f) $S = \mathbb{Z} \times \mathbb{N}$, $(a, b)R(c, d) \iff ad = bc$.

(10) Let R be an equivalence relation on a set S. Recall that for $x \in S$ the equivalence class $[x]$ of x is defined by

$$[x] = \{y \in S \mid yRx\}$$

Show carefully that if $[x] \cap [y] \neq \emptyset$ then $[x] = [y]$. [Hint: First show xRy. Then show $[x] \subset [y]$ and $[y] \subset [x]$, so $[x] = [y]$.]

(11) For each of the relations R in Q9 which are equivalence relations, describe the equivalence classes explicitly. [Hint: Recall that the equivalence classes of an equivalence relation R on a set S give a partition of the set S. Make sure your answer has this property!]

(12) Express the repeating decimal $0.131313\cdots$ as a fraction. [Hint: Recall that the meaning of a decimal expansion $x = 0.a_1a_2a_3\cdots$, where $a_1, a_2, a_3, \ldots \in \{0, 1, \ldots, 9\}$ are the digits, is $x = \sum_{n=1}^{\infty} a_n \cdot 10^{-n}$. Now use the formula $\sum_{n=0}^{\infty} r^n = 1/(1-r)$ for the sum of a geometric series with common ratio r such that $|r| < 1$.]

(13) For each of the following functions, compute the inverse or prove that no inverse exists.

(a) $f\colon \{1, 2, 3\} \to \{A, B, C\}$, $1 \mapsto B$, $2 \mapsto C$, $3 \mapsto A$.

(b) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 5x - 2$.

(c) $f\colon [2, \infty) \to [3, \infty)$, $f(x) = x^2 - 2x + 3$. [Hint: Use the quadratic formula.]

(d) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + 5x^2$.

(e) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 3x + 5$.

(f) $f\colon [0, 2\pi] \to [-1, 1]$, $f(x) = \cos(x)$.

(g) $f\colon (-\pi/2, \pi/2) \to \mathbb{R}$, $f(x) = \tan(x)$.

(14) Let $f\colon X \to Y$ be a function. What does it mean to say that f is injective? What does it mean to say that f is surjective? (Give precise definitions.)

(a) Show that if $f\colon X \to Y$ is injective and $X \neq \emptyset$ then there exists a surjective function $g\colon Y \to X$. [Hint: construct a function g such that $g(f(x)) = x$ for all $x \in X$.]

(b) Show that if $f\colon X \to Y$ is surjective then there exists an injective function $g\colon Y \to X$. [Hint: construct a function g such that $f(g(y)) = y$ for all $y \in Y$.]

(15) Let X, Y, Z be sets and $f\colon X \to Y$, $g\colon Y \to Z$ be functions. Define the composite function $g \circ f\colon X \to Z$.

(a) Show that if f is surjective and g is surjective then $g \circ f$ is surjective.

(b) Show that if $g \circ f$ is injective then f is injective.

(c) Give an example of two functions $f\colon X \to Y$ and $g\colon Y \to Z$ such that $g \circ f$ is injective but g is not injective.

(16) For each of the following pairs of sets X and Y, describe a bijection $f\colon X \to Y$ or prove that no such bijection exists.

(a) $X = \mathbb{N}$, $Y = \{n \in \mathbb{N} \mid n \geq 5\}$.

(b) $X = \mathbb{N}$, $Y = \{n \in \mathbb{N} \mid n \equiv 3 \bmod 4\}$.

(c) $X = \mathbb{N}$, $Y = \mathbb{N} \times \mathbb{N}$.

(d) $X = \mathbb{Z}$, $Y = \mathbb{R}$.

(e) $X = [0, 1]$, $Y = [3, 7]$. [Hint: Use a linear function $f(x) = mx + c$ where $m, c \in \mathbb{R}$ are to be determined.]

(f) $X = (0, 1)$, $Y = \mathbb{R}$. [Hint: First construct a bijection from $(0, 1)$ to $(-\pi/2, \pi/2)$, similarly to part (e). Then use Q13(g)].

(g) $X = \mathbb{Q}$, $Y = (0, 1)$.

(17) Let X and Y be countable sets.

(a) Show that $X \cup Y$ is countable. [Hint: Recall that if Z is a set and $f\colon \mathbb{N} \to Z$ is a surjection, then there exists a bijection $g\colon \mathbb{N} \to Z$ (why?), that is, Z is countable. So it suffices to construction a surjection from $\mathbb{N}$ to $X \cup Y$.]

(b) Show that $X \times Y$ is countable.