CS 70 Discrete Mathematics and Probability Theory
Fall 2011 Rao Midterm 1 Q3 Soln

1. (8 pts.) Quantifiers

(a) $(\forall n \in \mathbb{N})(P(n))$
D - If P is a statement which is always true, this proposition holds. If P is sometimes false, this statement will not hold.

(b) $(P(0) \wedge P(1)) \rightarrow ((\forall n \in \mathbb{N})(n \geq 1 \rightarrow P(n)))$
D - If P is a statement which is always true, this proposition could hold. If P is sometimes false, this statement will not hold. The base cases are insufficient to show the proposition holds for any values of n except powers of 2.

(c) $((\forall n \in \mathbb{N})(n \text{ is odd} \rightarrow P(n))) \rightarrow ((\forall n \in \mathbb{N})(n \geq 1 \rightarrow P(n)))$
T - If $P(n)$ holds for all odd n, it must hold for all $n \in \mathbb{N}$, because every n is either itself odd or a power of 2 multiplied by an odd number.

(d) $(\forall n \in \mathbb{N})(P(2n))$
D - If P is a statement which is always true for even n, this proposition holds. If P is sometimes false, this statement will not hold.

2. (13 pts.) True or False

(a) True
For $n \leq 3, \neg(n > 3)$, so $\neg(n > 3 \wedge n^2 < 16)$. For $n \geq 4, n^2 \geq 16$, so $\neg(n^2 < 16)$, so $\neg(n > 3 \wedge n^2 < 16)$.

(b) True
False statements may imply anything. Hence if P is false, $P \implies Q$. If Q is false, $Q \implies P$. If both P and Q are true, then $P \implies Q$, so for any boolean values of P, Q, the proposition is true.

(c) False
Let P, Q be false and R be true. Then $(P \wedge Q) \vee R$ is true but $(P \wedge R) \vee (Q \wedge R)$ is false.

(d) False
If $x + 7 \equiv y + 7 \pmod 9$ then $x \equiv y \pmod 9$

(e) True
$4x \equiv y \pmod 9 \implies$
$7 \times 4x \equiv 7 \times y \pmod 9 \implies$
$28x \equiv 7y \pmod 9 \implies$
$27x + x \equiv 7y \pmod 9 \implies$
$(3 \times 9)x + x \equiv 7y \pmod 9 \implies$
$x \equiv 7y \pmod 9$

(f) True
We know gcd(x,y) = gcd(y-x, x), so gcd(453,368) = gcd(453-368, 368) = gcd(85,368).

(g) True
If gcd$(x, m) = d$, $d > 1$, then choose $k = \frac{m}{d}$. $k \in \{1, 2, \ldots, m-1\}$. x can be written as $a \times d$, $d \in \mathbb{N}$. So, $kx \equiv adk \equiv am \equiv 0 \pmod m$.

(h) False
Choose $x = 1$. Then $\forall k \in \{1, 2, \ldots, p-1\}, kx \equiv k \pmod p \not\equiv 0 \pmod p$

(i) False
P and Q may each have up to 5 roots (x-values such that $P(x) = 0$). $P(x) \cdot Q(x)$ will have all the roots of both P and Q. If they had different roots, $(P \cdot Q)(x)$ could have up to 10 roots.

(j) True
If each of two polynomials contains 5 of 8 predetermined points, then they must share at least 2 points. It is possible to construct two different degree-3 polynomials which share 2 points.

(k) False
If each of two polynomials contains 6 of 8 predetermined points, then they must share at least 4 points. It is impossible to construct two different degree-3 polynomials which share 4 points.

(l) False
If each of two polynomials contains 7 of 8 predetermined points, then they must share at least 6 points. It is possible to construct two different degree-3 polynomials which share 6 points.

(m) False
Let man A's preferences for women be 1, 2. Let man B's preferences for women be 2, 1. Let woman 1's preferences for men be A, B. Let woman 2's preferences for men be B, A. The only stable pairing is (1, A), (2, B). Since it is the only pairing, it is pessimal for both women, though both women are not paired with their least favorite man.

3. (54 pts.) How many? What expression?

(a) $4! \cdot 2! \cdot 2!$.
There are 4! ways to choose the first row, 2! ways to choose the second row of the leftmost 2×2 subgrid, and 2! ways to choose the second row of the rightmost 2×2 subgrid.

(b) $\binom{6}{2} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$.
There are $\binom{6}{2}$ choices for the positions of the repeated dice (out of six rolls), 6 choices for the repeated value, and $5 \cdot 4 \cdot 3 \cdot 2$ choices for the remaining unique values.

(c) $\frac{n(n-3)}{2}$ or $\binom{n}{2} - n$.
The first answer comes from n choices for an endpoint u of a diagonal, and $n-3$ choices for the other endpoint of the diagonal (excluding the vertex u itself and its two neighbors). Divide this number by 2 for having doubly counted each diagonal.
The second answer comes from $\binom{n}{2}$ choices for two distinct vertices, and subtracting the n choices for adjacent pairs that aren't diagonal.

(d) $\binom{n}{k}$.
A subset of k (distinct) integers from $\{1,\ldots,n\}$ corresponds uniquely to an increasing sequence of k integers from $\{1,\ldots,n\}$, and vice versa. (Sort the k integers in a subset to get an increasing sequence.)

(e) $\binom{n+k-1}{k}$.
A configuration of k balls inside n bins corresponds uniquely to a nondecreasing sequence of k integers from $\{1,\ldots,n\}$, and vice versa. (A ball in bin i corresponds to an occurrence of the integer i in a nondecreasing sequence.)
A common incorrect answer is $n^k - \binom{n}{k}$, which is the number of "not decreasing" sequences of k integers from $\{1,\ldots,n\}$. This is incorrect because a "not decreasing" sequence need not be nondecreasing.

(f) p^{d+1}.
In a polynomial $c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d$ of degree at most d, there are p choices for each of the $d+1$ coefficients $c_0,\ldots,c_d$.

(g) $\binom{p}{d}(p-1)$.
There are $\binom{p}{d}$ choices for d distinct roots $a_1,\ldots,a_d$, and $p-1$ choices for the non-zero value $P(b)$ at any other point b. The polynomial is then uniquely determined by the $d+1$ points $(a_1,0),\ldots,(a_d,0)$ and $(b,P(b))$.

(h) 0.
By Langrange interpolation formula, $P(x) = 2 \cdot \Delta_1(x) + 1 \cdot \Delta_2(x) + 0 \cdot \Delta_3(x)$, where

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{x^2-5x+6}{2} \qquad \Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = \frac{x^2-4x+3}{-1}. \tag{1}$$

(Recall that all arithmetics are $\bmod 5$.) Plugging (1) into the above formula, the coefficient of x^2 in $P(x)$ is $2 \cdot 2^{-1} + 1 \cdot (-1) = 0$.

(i) 0.
This is a special case of part (k) below with $m = 12, n = 4, b = 6$.

(j) 4.
This is a special case of part (l) below with $m = 12, n = 8, b = 4$.

(k) 0.
As x runs over $\{0,\ldots,m-1\}$, nx runs over multiples of d. nx is never equivalent to any integer b that is not a multiple of d.

(l) d.
As x runs over $\{0,\ldots,m-1\}$, nx runs over multiples of d. There are m/d such multiples from $\{0,\ldots,m-1\}$, and nx is equivalent to any multiple b exactly d times.

(m) 7.
By Fermat's Little theorem, $15^{36} \equiv 1 \pmod{37}$. Hence $15^{404} = (15^{36})^{11} \cdot 15^8 \equiv 1^{11} \cdot 15^8 = 15^8 \pmod{37}$. To compute $15^8 \pmod{37}$, we use repeated squaring, yielding $15^2 = 225 \equiv 3 \pmod{37}$, $15^4 \equiv 3^2 = 9 \pmod{37}$, $15^8 \equiv 9^2 = 81 \equiv 7 \pmod{37}$.

(n) 9.
In the analysis of RSA, we proved $x^{1+(p-1)(q-1)} \equiv x \pmod{pq}$ for any distinct primes p,q. Apply it with $p = 5, q = 7$, we get $(9^5)^5 = 9^{1+(5-1)(7-1)} \equiv 9 \pmod{35}$.

(o) 0.
$1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + (p-1) \pmod{p}$, by applying Fermat's little theorem to each summand. Now $1+2+\cdots+(p-1) = p(p-1)/2$, which is equivalent to $0 \pmod{p}$, since $(p-1)/2$ is an integer when p is an odd prime.

(p) 2.
If Jung Lin isn't proposed on the first day, some other woman is proposed by multiple men on that day, and some man gets rejected. That man will propose to Jung Lin on the second day.

(q) $n+2$.
At least one man gets rejected every day (except the last). During the first $n+1$ days, some man must be rejected at least twice. That man will propose to Sheila on day $n+2$ (or earlier). It is possible to come up with preference lists so that Sheila is first proposed on day $n+2$ (by having exactly one man rejected every day, and having exactly one man rejected more than once in the first $n+1$ days).

(r) T.
Some woman is proposed every day during a run of TMA.

4. (25 pts.) Reviewing Simple Proofs

Solution to 4a:

Proof by contradiction: Assume that $\sqrt{3}$ is rational. This means there are integers a and b (with $b \neq 0$) such that $\sqrt{3} = \frac{a}{b}$. Without loss of generality, we shall furthermore require that a and b are positive and in lowest terms; that is, they have been selected so that $\gcd(a,b) = 1$.

Squaring both sides of $\sqrt{3} = \frac{a}{b}$ gives us $3 = \frac{a^2}{b^2}$, which is to say, $3b^2 = a^2$. This means that 3 divides a^2. Since 3 is prime, the lemma tells us that 3 also divides a. So let k be an integer such that $a = 3k$. By substituting this in, we get $3b^2 = (3k)^2 = 9k^2$. So $b^2 = 3k^2$. So 3 divides b^2, which by the lemma again, means 3 divides b.

Thus, 3 must be a common factor of a and b. But this contradicts the assumption that $\gcd(a,b) = 1$. So $\sqrt{3}$ cannot be written as a ratio of positive integers in lowest terms, and therefore, is not rational.

Alternative solution to 4a (there are many ways to present the same underlying idea):

As before, assume, for the sake of a contradiction, that there are positive integers a and b such that $\sqrt{3} = \frac{a}{b}$, which is to say, $a^2 = 3b^2$.

Let e_a be the exponent of 3 in the prime factorization of a and let e_b be the exponent of 3 in the prime factorization of b.

Note that the exponent of 3 in the prime factorization of a^2 is $2e_a$, which is even. But the exponent of 3 in the prime factorization of $3b^2$ is $1 + 2e_b$, which is odd. Since a^2 was assumed to equal $3b^2$ (and every positive integer has a *unique* prime factorization), we have reached a contradiction, and can conclude $\sqrt{3}$ is irrational.

Solution to 4b:

Proof by induction:

Base Case: $n = 0$. In this case, $3^{n+1} = 3^{0+1} = 3$ and $2^{3^n} + 1 = 2^{3^0} + 1 = 2^1 + 1 = 3$. 3 divides 3.

Inductive step: Let n be some nonnegative integer. Assume that 3^{n+1} divides $2^{3^n} + 1$. Now our goal will be to show that 3^{n+2} divides $2^{3^{n+1}} + 1$.

Since 3^{n+1} divides $2^{3^n} + 1$, there is some integer k so that $2^{3^n} + 1 = k \cdot 3^{n+1}$. So $2^{3^n} = k \cdot 3^{n+1} - 1$. Now

$$\begin{aligned} 2^{3^{n+1}} + 1 &= \left(2^{3^n}\right)^3 + 1 = \left(k \cdot 3^{n+1} - 1\right)^3 + 1 = k^3 \cdot 3^{3n+3} - 3 \cdot k^2 \cdot 3^{2n+2} + 3 \cdot k \cdot 3^{n+1} - 1 + 1 \\ &= 3^{n+2}\left(k^3 \cdot 3^{2n+1} - k^2 \cdot 3^{n+1} + k\right) \end{aligned}$$

So 3^{n+2} divides $2^{3^{n+1}} + 1$ as required to complete the induction. =