**Math 55: Discrete Mathematics, Fall 2008**
**Final Exam Solutions**

1. Does there exist a 1-to-1 and onto function from the set of positive integers to the set of all integers? If so, construct one. If not, explain why not.

An example of such a function is

$$f(n) = \begin{cases} (n-1)/2 & \text{if } n \text{ is odd,} \\ -n/2 & \text{if } n \text{ is even,} \end{cases}$$

since this function maps the odd positive integers 1-to-1 onto $\{0, 1, 2, \ldots\}$ and the even postivie integers 1-to-1 onto $\{-1, -2, -3, \ldots\}$.

2. (a) Given the information that $2^{23376} \equiv 1 \pmod{23377}$, what, if anything, can you conclude about whether 23377 is prime?

(b) How would your answer change given the additional information that $2^{11688} \equiv 15907 \pmod{23377}$? [Note that $11688 = 23376/2$.]

In part (a), 23377 passes the Fermat test to the base 2. No conclusion can be drawn from this information.

In part (b), 23377 fails Miller's test, since $2^{11688} \not\equiv \pm 1 \pmod{23377}$. This implies that 23377 is composite. (In fact, $23377 = 97 \times 241$.)

3. Prove that in any set of ten integers there are two that differ by a multiple of 9.

By the pigeonhole principle, two of the ten integers must be in the same conguence class mod 9.

4. A biased coin has probability 1/3 of coming up heads on each flip. Let the random variable $X$ be the number of heads seen in 99 independent flips of the coin.

(a) Find the expectation $EX$.

(b) Find the variance $V(X)$.

(c) Use the expectation and variance of $X$ to find an upper bound on $P(X \geq 40)$.

(a,b) If $X_i$ is the indicator variable for heads on the $i$-th flip, then $EX_i = 1/3$, and $V(X_i) = 2/9$. By linearity of expectation, $EX = 99(1/3) = 33$. By addititivity of independent variances, $V(X) = 99(2/9) = 22$.

(c) $P(X \geq 40) \leq P(|X - 33| \geq 7) = P(|X - EX| \geq 7) \leq V(X)/7^2 = 22/49$, by Chebyshev's inequality.

5. Consider the linear code over $\mathbb{Z}_2$ given by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(a) Find the minimum weight of a non-zero codeword in this code.

(b) How many errors can this code correct?

(c) Can this code detect more errors than it can correct?

(a) Minimum weight = 5. (Each row of the matrix has weight 6 or 7, each sum of two rows has weight 5 or 6, and the sum of all three rows has weight 5.)

(b,c) It can correct 2 errors and cannot detect more than 2 errors.

6. Find the number of permutations of the 26 letters of the alphabet that do not contain any of the strings RUN, WALK, or SWIM in consecutive positions.

Let $A_{\mathrm{RUN}}$, $A_{\mathrm{WALK}}$, $A_{\mathrm{SWIM}}$ be the sets of permutations containing the given strings. Thinking of the strings as single letters, we get $|A_{\mathrm{RUN}}| = 24!$, $|A_{\mathrm{WALK}}| = |A_{\mathrm{SWIM}}| = 23!$, and $|A_{\mathrm{RUN}} \cap A_{\mathrm{WALK}}| = |A_{\mathrm{RUN}} \cap A_{\mathrm{SWIM}}| = 21!$. Other intersections are empty, since W is in both SWIM and WALK. By inclusion-exclusion, the result is

$$26! - 24! - 2 \cdot 23! + 2 \cdot 21!$$

7. Consider the relation on the set of integers defined by $x \sim y$ if $x^2 \equiv y^2 \pmod 5$.

(a) Show that $\sim$ is an equivalence relation.

(b) Find its equivalence classes.

(a) The reflexive and symmetric properties are obvious, and the transitive property holds because $x^2 \equiv y^2 \equiv z^2 \pmod 5$ implies $x^2 \equiv z^2 \pmod 5$.

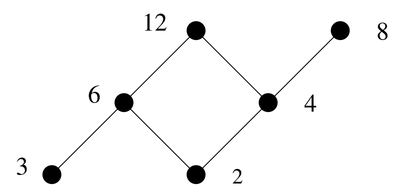
(b) There are three equivalence classes: $\{x \equiv 0 \pmod 5\}$, $\{x \equiv \pm 1 \pmod 5\}$, and $\{x \equiv \pm 2 \pmod 5\}$.

8. Let $P$ be the set of integers $\{2, 3, 4, 6, 8, 12\}$, partially ordered by the divisibility relation $x \mid y$.

(a) Draw the Hasse diagram of $P$.

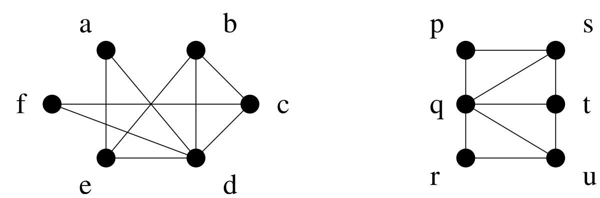
(b) Find the number of extensions of $P$ to a compatible linear ordering.

(a)




(b) There are 14 compatible extensions.

9. Either find an isomorphism between the two graphs shown below, or show that none exists.



One isomorphism is $(a, b, c, d, e, f) \mapsto (p, t, u, q, s, r)$. Another is $(a, b, c, d, e, f) \mapsto (r, t, s, q, u, p)$.

10. Prove that for all $n \geq 4$, the Stirling number $S(n, n-2)$ is given by the formula

$$S(n, n-2) = \binom{n}{3} + \frac{1}{2}\binom{n}{2, 2, n-4}.$$

By definition, $S(n, n-2)$ is the number of partitions of an $n$-element set into $n-2$ blocks. Such partitions are of two types: (i) one block of size 3 and $n-3$ singletons, or (ii) two blocks of size 2 and $n-4$ singletons. The number of partitions of type (i) is $\binom{n}{3}$, while that of type (ii) is $\frac{1}{2}\binom{n}{2,2,n-4}$. We divided by 2 here because there is no ordering on the two 2-element blocks in type (ii).