CMSC-37110 Discrete Mathematics
SOLUTIONS TO SECOND MIDTERM EXAM
November, 2005

Instructor: László Babai Ryerson 164 e-mail: `laci@cs`

This exam contributes 20% to your course grade.

1. (6 points) Let $a_n, b_n > 1$. Prove that the condition $a_n \sim b_n$ does NOT imply $a_n^n = \Theta(b_n^n)$. Before giving your counterexample, state clearly what properties your counterexample needs to have, and prove that it indeed has those properties.

   Answer. We need to give an example of two sequences $a_n, b_n > 1$ such that $a_n \sim b_n$ but all c and all sufficiently large n, either $a_n^n > cb_n^n$ or $b_n^n > ca_n^n$.

   Example: $a_n = n^{1/n}$; $b_n = n^{2/n} = a_n^2$. Now $a_n \to 1$ because $\ln a_n = \ln n/n \to 0$; therefore $b_n/a_n = a_n \to 1$, so $a_n \sim b_n$. On the other hand, $b_n^n/a_n^n = a_n^n = n$ is unbounded, therefore $b_n^n \neq O(a_n^n)$ and consequently $b_n^n \neq \Theta(a_n^n)$.

2. (4+4+6+3+6+4 points)

   (a) Define the relation $a_n = \Omega(b_n)$. Do not use the big-Oh notation. Give a properly quantified formula, no English words.

   Answer. $(\exists c > 0)(\exists n_0)(\forall n \geq n_0)(|a_n| \geq c|b_n|)$.

   (b) True or false? $F_{n+1} = O(F_n)$ (Fibonacci numbers). Give a simple proof of your answer.

   Answer. TRUE. We **claim** that $F_{n+1} \leq 2F_n$ and therefore $F_{n+1} = O(F_n)$.

   Proof of the Claim. For $n \geq 0$ we have $F_n \geq 0$ (by induction). Therefore, for $n \geq 2$ we have $F_n = F_{n-1} + F_{n-2} \geq F_{n-1}$. Consequently, $F_{n+1} = F_n + F_{n-1} \leq 2F_n$.

   (c) Prove: if $a_n = \Theta(b_n)$ and $a_n \to \infty$ then $\ln(a_n) \sim \ln(|b_n|)$.

   Answer. We know that $(\exists c > 0, C, n_0)$ such that for all $n \geq n_0$ we have

   $$ca_n \leq |b_n| \leq Ca_n. \quad (1)$$

   Taking logarithms,

   $$\ln c + \ln a_n \leq \ln |b_n| \leq \ln C + \ln a_n. \quad (2)$$

   Dividing by the positiv quantity a_n,

   $$\frac{\ln c}{\ln a_n} + 1 \leq \frac{\ln |b_n|}{\ln a_n} \leq \frac{\ln C}{\ln a_n}. \quad (3)$$

By assumption, $\frac{\ln c}{\ln a_n} \to 0$ and $\frac{\ln C}{\ln a_n} \to 0$. Therefore the fraction $\frac{\ln |b_n|}{\ln a_n}$ is between two sequences both of which converge to 1. By the "squeeze principle" (a.k.a. "sandwich principle") the fraction in the middle also approaches 1, i. e., $\ln(a_n) \sim \ln(|b_n|)$.

(d) True or false: $\ln x = \Theta(\log_2 x)$. Prove your answer.

Answer. TRUE. $\ln x = c \log_2 x$ where $c = \ln 2$.

(e) True or false: $\pi(x) = \Omega(x^{0.9})$, where $\pi(x)$ is the number of primes $\leq x$.

Answer. TRUE. Equivalently, $x^{0.9} = O(\pi(x))$. In fact, the stronger statement $x^{0.9} = o(\pi(x))$ is true. Reason:

$$\frac{x^{0.9}}{\pi(x)} \sim \frac{x^{0.9}}{x/\ln x} = \frac{\ln x}{x^{0.1}} \to 0. \tag{4}$$

(f) Prove: $\ln(x^5 + 5x^2 - 100) = \Theta(\ln(4x^9 - 5x^2 + 1))$.

Answer. Let $f(x)$ be a polynomial of degree $n \geq 1$ with positive leading coefficient. Then, for all sufficiently large x,

$$\sqrt{x} < f(x) < x^{n+1} \tag{5}$$

(because $\sqrt{x} = o(f(x))$ and $f(x) = o(x^{n+1})$). Taking logarithms,

$$(1/2)\ln x < \ln f(x) < (n+1)\ln x \tag{6}$$

hold for all sufficiently large x. Therefore $\ln(f(x)) = \Theta(\ln x)$. It follows that for any two polynomials $f_1(x)$ and $f_2(x)$ of degrees ≥ 1 with positive leading coefficients, the logarithm of each polynomial is $\Theta(\ln x)$ and therefore, by the transitivity of the Θ relation, $\ln(f_1(x))$ and $\ln(f_2(x))$ are in Θ relation with each other.

3. (6+3B points) For the positive integer x, let $n(x)$ denote the number of decimal digits of x. (a) Prove: $n(x) \sim \lg(x)$ where lg refers to base-10 logarithms. (b) BONUS: give a very simple explicit formula for $n(x)$ in terms of the lg function and the rounding (floor or ceiling) functions.

Answer. (a) The key observation is that $10^{n(x)-1} \leq x < 10^{n(x)}$. Taking logarithms, it follows that

$$n(x) - 1 \leq \lg x < n(x). \tag{7}$$

Dividing by $n(x)$ we obtain

$$1 - \frac{1}{n(x)} \leq \frac{\lg x}{n(x)} < 1. \tag{8}$$

Since $1/n(x) \to 0$, we obtain, as before by the Squeeze Principle, that $\lg x/n(x) \to 1$, proving that $n(x) \sim \lg x$.

(b) The inequalities (7) are equivalent to saying that $n(x) - 1 = \lfloor \lg x \rfloor$ and therefore $n(x) = 1 + \lfloor \lg x \rfloor$. Another correct formula is: $n(x) = \lceil \lg(x+1) \rceil$. (Why?)

4. **(A:3+3, B:5+5B points)** Give simple closed-form expressions of the (a) ordinary generating function (b) exponential generating function of the sequences (A) $1, -1, 1, -1, \dots$ and (B) $1, 0, 0, 1, 0, 0, 1, 0, 0, \dots$. (bB) is a bonus problem.

   Answer. Observing that $1/(1-z) = \sum_{i=0}^{\infty} z^i$, and setting $z = qx$, we obtain that for the geometric progression $1, q, q^2, \dots$, the (ordinary) generating function is $1/(1-qx)$. From the Taylor series $\mathrm{e}^z = \sum_{i=0}^{\infty} z^i/i!$ we obtain, again by setting $z = qx$, that for the same geometric progression, the exponential generating function is e^{qx}. Setting $q = -1$ we obtain $1/(1+x)$ for (Aa) and e^{-x} for (Ab). Setting $z = x^3$ in our first formula we see that the answer to (Ba) is $1/(1-x^3)$. – (Bb) is left as a challenge problem.

5. **(6 points)** Give a simple closed-form expression for the ordinary generating function of the Fibonacci numbers ($F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$). Show all your work.

   Answer. (done in class)

6. **(5 points)** Pick a random integer from $\{1, 2, \dots, 101\}$. Let A be the event that x is even; and B the event that $3 \mid x$. Are the events A and B positively correlated, negatively correlated, or independent?

   Answer. $\lfloor 101/2 \rfloor = 50$; $\lfloor 101/3 \rfloor = 33$; $\lfloor 101/6 \rfloor = 16$; therefore $P(A) = 50/101$, $P(B) = 33/101$, $P(A \cap B) = 16/101 < (50/101) \cdot (33/101)$ because $1616 = 16 \cdot 101 < 50 \cdot 33 = 1650$. Therefore A and B are negatively correlated.

7. **(4+4 points)** (a) Calculate the largest k such that 3^k divides $83!$ (83-factorial). (b) Calculate the largest ℓ such that 3^ℓ divides $\binom{83}{21}$. Do NOT use calculator for this question; show all your work.

   Answer. (a) Let $k_p(n)$ denote the exponent in the largest power of p that divides $n!$. Then the question is $k = k_3(83)$.

$$k_3(83) = \left\lfloor \frac{83}{3} \right\rfloor + \left\lfloor \frac{83}{3^2} \right\rfloor + \left\lfloor \frac{83}{3^3} \right\rfloor + \left\lfloor \frac{83}{3^4} \right\rfloor = 27 + 9 + 3 + 1 = 40. \quad (9)$$

   (b) The desired exponent is $\ell = k_3(83) - k_3(21) - k_3(62) = (27 + 9 + 3 + 1) - (7 + 2) - (20 + 6 + 2) = 0 + 1 + 1 + 1 = 3$.

8. **(6 points)** Prove: $(\forall x)(x^{13} \equiv x \pmod{65})$.

Answer. $65 = 5 \cdot 13$ and 5 and 13 are relatively prime so it suffices to prove the congruence modulo 5 and modulo 13 separately. (a) By Fermat's Little Theorem, if $13 \nmid x$ then $x^{12} \equiv 1 \pmod{13}$ and therefore $x^{13} \equiv x \pmod{13}$. But this last congruence also holds if $13 \mid x$ since then both sides are $\equiv 0 \pmod{13}$. (b) If $5 \nmid x$ then $x^4 \equiv 1 \pmod{5}$; therefore $x^{12} = (x^3)^4 \equiv 1^4 = 1 \pmod{5}$ and consequently $x^{13} \equiv x \pmod{5}$. But the last congruence also holds when $5 \mid x$ because then both sides are $\equiv 0 \pmod{13}$.

9. **(4+2B points)** (a) Let $x > 0$. Show that the largest term in the Taylor series $\mathrm{e}^x = \sum_{n=0}^{\infty} x^n/n!$ occurs when $n = \lfloor x \rfloor$. (b) (BONUS) Prove, using the Taylor series of e^x, that $n! > (n/\mathrm{e})^n$. (Hint: find the largest term of the expansion of e^n. Do not use Stirling's formula.)

Answer. (a) Let $a_n = x^n/n!$ be the n-th term of the series. Consider the quotient of two consecutive terms:

$$\frac{a_n}{a_{n-1}} = \frac{x^n/n!}{x^{n-1}/(n-1)!} = \frac{x}{n}. \tag{10}$$

So as long as $x \geq n$, we have $a_n \geq a_{n-1}$; after that, $a_n < a_{n-1}$. So the largest term occurs for the greatest n such that $n \leq x$; this is $n = \lfloor x \rfloor$.

(b) $n^n/n!$ is one of the terms (in fact, the largest term) in the expansion of e^n, therefore $\mathrm{e}^n > n^n/n!$. Rearranging the inequality we obtain $n! > (n/\mathrm{e})^n$.

10. **(6 points)** Decide whether or not the following system of congruences is solvable. Prove your answer.

$x \equiv 2 \pmod{9}$

$x \equiv 8 \pmod{21}$

$x \equiv 1 \pmod{7}$

Answer. (First solution) $7 \mid 21$, so the second congruence implies the third, therefore the third congruence is redundant: x satisfies all the three congruences if and only if it satisfies the first two. The second congruence is equivalent to the pair of congruences $x \equiv 8 \pmod{7}$ and $x \equiv 8 \pmod{3}$, or equivalently, $x \equiv 1 \pmod{7}$ and $x \equiv 2 \pmod{3}$. The last congruence follows from $x \equiv 2 \pmod{9}$ and therefore is redundant. So the entire system is equivalent to the pair of congruences $x \equiv 2 \pmod{9}$ and $x \equiv 1 \pmod{7}$. By the Chinese Remainder Theorem, this system (and therefore the original system) has a unique solution modulo 63.

(Second solution: by guessing) The positive solutions to the second congruence are $8, 29, 50, \ldots$. Luckily we can observe that 29 satisfies all the three congruences; therefore a solution exists. It also follows that the solution is unique modulo the l.c.m.$(9, 21, 7) = 63$.

11. (2+6+9 points) A careless secretary puts n distinct letters into n addressed envelopes at random. All addresses are different. Let X denote the number of letters that happen to get in the right envelope. (a) What is the size of the sample space of this experiment? (b) Determine $E(X)$. If you use auxiliary random variables, define them clearly. Half the credit goes for this definition. (c) Determine the probability that $X = 0$ (none of the letters goes in the right envelope). Name the method used. Prove that this probability approaches 1/e as $n \to \infty$.

   Answer. (a) $n!$ (b) Let Y_i be the indicator variable of the event A_i that letter $\#i$ got in the right envelope. Then $X = \sum_{i=1}^{n} Y_i$ and therefore $E(X) = \sum_{i=1}^{n} E(Y_i)$. Now $E(Y_i) = P(A_i) = 1/n$ and therefore $E(X) = \sum_{i=1}^{n} 1/n = n \cdot (1/n) = 1$.

12. (5B points) (BONUS) Prove that the Fibonacci sequence modulo m is periodic and the period is not longer than $m^2 - 1$. Example: the Fibonacci sequence modulo 3 is $0, 1, 1, 2, 0, 2, 2, 1$, repeat. The length of the period is $8 = 3^2 - 1$.

   Answer. Remains a challenge problem.

13. (2+4+B5 points) Let $V = \{1, 2, \ldots, n\}$, $n \geq 3$. Let us consider a random graph $\mathcal{G}$ on the vertex set V; adjacency is decided by coin flips. (a) What is the size of the sample space for this experiment? (b) Let A_i denote the event that vertex i has even degree. What is the probability of A_i?

   Answer. (a) $2^{\binom{n}{2}}$. (b) Let j be a vertex other than i. There is a 1-to-1 correspondence between those outcomes of the experiment where the degree of i is even and those where the degree of i is odd: just flip the coin deciding the adjacency of i and j. Therefore $P(A_i) = 1/2$.

   (c) BONUS PROBLEM. What is the probability that all vertices of $\mathcal{G}$ have even degree?

   Answer. Remains a challenge problem.

14. (6 points) Find the multiplicative inverse of 62 modulo 91. Your answer should be an integer between 1 and 90. Show all your work.

   Answer. We follow the steps of Euclid's algorithm, starting from the conditions (a) $62x \equiv 1 \pmod{91}$ and (b) $91x \equiv 0 \pmod{91}$. Subtracting (a) from (b), we obtain (c) $29x \equiv -1 \pmod{91}$. Now we subtract 2(c) from (a) and obtain (d) $4x \equiv 3 \pmod{91}$. Finally we subtract

7(d) from (c) and obtain $x \equiv -22 \equiv 69 \pmod{91}$. So if there is a solution, it can only be $x \equiv 69 \pmod{91}$. We also proved in the process that $\gcd(62, 91) = 1$ (we executed Euclid's algorithm on the coefficient of x), so a solution indeed must exist.

15. (5B points) (BONUS) Prove: $\gcd(2^k - 1, 2^\ell - 1) = 2^d - 1$, where $d = \gcd k, \ell$. (Hint: induction on $k + \ell$.)

    Answer. If $k = 0$ then we have $d = \ell$ and $\gcd(0, 2^\ell - 1) = 2^\ell - 1 = 2^d - 1$. Similarly if $\ell = 0$. Now we may assume $k, \ell \geq 1$ and assume that the statement is true for k', ℓ' if $k' + \ell' < k + \ell$. WLOG we may assume $k \geq \ell$.

    We know that $\gcd(a, b) = \gcd(a - b, b)$. Therefore $\gcd(2^k - 1, 2^\ell - 1) = \gcd(2^k - 2^\ell, 2^\ell - 1) = \gcd(2^\ell(2^{k-\ell} - 1), 2^\ell - 1) = \gcd(2^{k-\ell} - 1, 2^\ell - 1)$. (We were able to omit the term $2^{k-\ell}$ because $2^\ell - 1$ is odd.) We can now use the inductive hypothesis, so the right-hand side is $2^s - 1$ where $s = \gcd(k - \ell, \ell) = \gcd(k, \ell)$.

16. (4+6+6B points)

    (a) Prove: there are infinitely many prime numbers. Give Euclid's proof.

    Answer. Assume, for a contradition, that $p_1, \ldots, p_n$ is a complete list of all primes. Consider the number $N = \prod_{i=1}^n p_i + 1$. Then, for every i we have $N \equiv 1 \pmod{p}_i$. Let now p be a prime divisor of N. Then $N \equiv 0 \pmod{p}$. On the other hand, p must be one of the p_i (the list being complete), so we have $N \equiv 1 \pmod{p}$ and therefore $1 \equiv 0 \pmod{p}$, a contradiction.

    (b) Prove: there are infinitely many prime numbers of the form $4k-1$. (Do not use Dirichlet's theorem.)

    Answer. Lemma. If $N > 1$ and $N \equiv -1 \pmod{4}$ then N has a prime divisor of the form $4k - 1$.
    Proof. Let $N = p_1 \ldots p_s$ where the p_i are (not necessarily distinct) primes. N is odd, so each p_i is odd. If all of them were $\equiv 1 \pmod{4}$ then so would be their product. So at least one of them must be $\equiv -1 \pmod{4}$, proving the Lemma.

    Proof of the result stated in the problem. Assume, for a contradiction, that $q_1, \ldots, q_t$ is a complete list of all primes $\equiv -1 \pmod{4}$. Consider the number $N = 4\prod_{i=1}^t q_i - 1$. So for each i we have $N \equiv -1 \pmod{q_i}$. Since $N \equiv -1 \pmod{4}$ and $N > 1$, it follows by the Lemma that N has a prime divisor q such that $q \equiv -1 \pmod{4}$. So $N \equiv 0 \pmod{q}$. On the other hand, q must be one of the q_i (the list being complete), so we have $N \equiv -1 \pmod{q}$ and therefore $-1 \equiv 0 \pmod{q}$, a contradiction.

(c) (BONUS) Prove: there are infinitely many prime numbers of the form $4k+1$. (Hint: use the fact that -1 is a quadratic nonresidue modulo primes of the form $4k-1$.)

Answer. Reamins a challenge problem.

17. (6 points) Count the 5-cycles in the complete graph K_n. A 5-cycle is a subgraph isomorphic to C_5.

Answer. K_5 has $4!/2 = 12$ 5-cycles: start at vertex 1, move to any one of 4 places, then to any of 3 places, then to 2, and finally 1. This gives 41 choices; but we counted every cycle twice (we can traverse them in two directions). So the total number of 5-cycles in K_n is $12\binom{n}{5}$.

18. (5B points) (BONUS) Pick a random integer x between 1 and n. Let $r(x)$ denote the number of distinct prime divisors of x (so $r(12) = 2$). Prove: $E(r(x)) \sim \ln\ln n$.

Answer. Remains a challenge problem.