AM 106: Applied Algebra **Prof. Madhu Sudan**

Problem Set 1

Assigned: Wed. Sept. 6, 2017 Due: Tue. Sept. 12, 2017 (11:59 PM)

- You may submit your solutions via assignment page on the canvas website of the course.
- For collaboration and late days policy, see course website at `http://madhu.seas.harvard.edu/courses/Fall2017`
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problem 1. (Induction) Consider the following one-dimensional variant of "Game of Life". The process starts at time 0 with one particle sitting at the origin $x = 0$. At each time step a particle at location $x = i$ splits into two particles with one placing itself at location $i + 1$ and the other at location $i - 1$. But if two particles attempt to place themselves at the same location, they annihilate and die. (See Figure below for an illustration.)

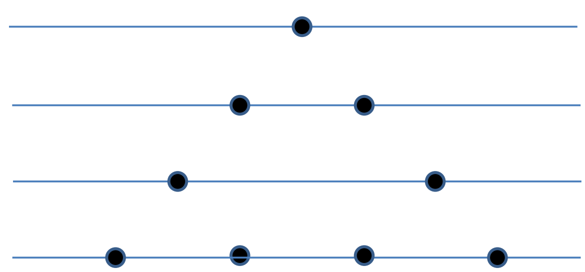

Figure 1: Particle evolution for 3 steps.

1. How many particles are there at time $t = 65536$? Prove your answer.
(**Hint:** Play with the particles to form a hypothesis about how the evolution goes. This hypothesis might need to be strengthened to make it suitable for induction. State the hypothesis clearly, and then prove it by induction.)
(**Warning:** This problem may be harder than the rest of this problem set - and if you are stuck it might be a good idea to do the other problems first and return to this at the end.)
2. (Extra credit, need not be turned in): Give a formula expressing the number of particles at time t for general t. (No need to prove your answer.)

Problem 2. (Equivalence Relations) Which of the following are equivalence relations? If it is an equivalence relation, describe the equivalence classes. If it is not, which properties fail?

1. Domain: the positive integers. Relation: $a \sim b$ if $\gcd(a, b) > 1$.
2. Domain: sets of real numbers. Relation: $A \sim B$ if $A \cap B = \emptyset$.
3. Domain: the complex numbers. Relation: $a \sim b$ if $a = rb$ for a positive real number r.

Problem 3. (Modular Exponentiation)

1. Show that there is no polynomial-time algorithm that, when given $x, y \in \mathbb{N}$, computes x^y. (Hint: how many bits/digits can x^y have?)
2. Give a polynomial-time algorithm that, when given $x, y, z \in \mathbb{N}$ with $z > 0$, computes $x^y \bmod z$. (Hint: use the formula $x^y = \prod_i (x^{2^i})^{y_i}$, where y_i is the i'th bit of the binary representation of y, and be careful about the length of intermediate values.)

Problem 4. (Subquadratic Integer Multiplication)

1. Given two $2n$-bit numbers $a, b \in \mathbb{N}$, we can write $a = a_u \cdot 2^n + a_\ell$ and $b = b_u \cdot 2^n + b_\ell$, where a_u, a_ℓ, b_u, b_ℓ are n-bit integers. Then the product $a \cdot b = a_u b_u \cdot 2^{2n} + a_u b_\ell \cdot 2^n + a_\ell b_u \cdot 2^n + a_\ell b_\ell$ can be computed using 4 multiplications of n-bit integers and 3 additions of $2n$-bit integers. Give a different way of computing the product that involves only 3 multiplications of $(n+1)$-bit integers and a constant number of additions of $2n$-bit integers.
2. Using the above, give an algorithm for multiplying n-bit integers in time $O(n^{\log_2 3}) = O(n^{1.59})$.

Problem 5. (Asymptotic Notation) True or False? Briefly justify your answers in one sentence each. Your answers should go back to the definitions of $O(\cdot)$, $\Omega(\cdot)$, and $\Theta(\cdot)$. For example, the definition of $O(\cdot)$ says that $f(n) = O(g(n))$ if there exist c and n_0 such that for every $n \geq n_0$ it is the case that $f(n) \leq c \cdot g(n)$. So, if the answer is true, give the values of c and n_0 such that the statement holds; Or if the answer is false, explain why no c or n_0 would work.

1. $5n + 6 = O(n)$.
2. $n^2 = O(n^3)$.
3. $n^2 = \Omega(n^3)$.
4. $n = O(\log^2 n)$.
5. $\ln n = \Theta(\log_2 n)$.
6. $5^n = 3^{O(n)}$.