AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Problem Set 4

Assigned: Sun. Sept. 19, 2010 Due: Fri. Sept. 24, 2010 (2:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS4-yourlastname`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.
- Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (Modular Exponentiation [AM106-B])

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 $x^y \bmod z$. Justify both the correctness and running time of your algorithm. (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 2. (Subquadratic Integer Multiplication [AM206-B])

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 $4n$-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 $4n$-bit integers.
2. Using the above, give an algorithm for multiplying n-bit integers in time $O(n^{\log_2 3}) = O(n^{1.59})$. Justify both the correctness and running time of your algorithm.

Problem 3. (Solving Equations via Euclid)

1. **[AM106-A]** Use the Extended Euclidean Algorithm to compute $\gcd(18900, 17017)$ and express it as an integer linear combination of 18900 and 17017. Show your work.

2. **[AM106-A]** Find an integer solution to the equation $18900x + 17017y = 14$.

3. **[AM206-A]** Provide a general characterization, in terms of the integers a,b, and c, for when there is an integer solution to the equation $ax + by = c$. Prove that your characterization is necessary and sufficient. Explain how it yields a polynomial-time algorithm for determining whether such an equation is solvable and, if so, finding a solution.

4. Prove by induction that if the Euclidean Algorithm makes k divisions when computing $\gcd(x, y)$, where $x > y \geq 1$ and $k \geq 1$, then $x \geq F_{k+2}$, where F_n is the n'th Fibonnaci number as defined on Problem 3 on PS0. Using Problem 3 of PS0, deduce that the number of divisions used when computing the gcd of two n-bit numbers is at most $(\log_\varphi 2) \cdot n \approx 1.44n$. (Note that this improves the bound of $2n$ given in lecture.)

Problem 4. (Groups) Which of the following are groups? For those that are finite groups write a Cayley table. Briefly justify your answers.

1. $\{0, 3, 6, 9\}$ with addition mod 12.

2. $\{1, 3, 5, 7, 9\}$ with multiplication mod 11.

3. The set of polynomials with rational coefficients (e.g. $(8/3)x^3 - 2x + 1/2$), under polynomial multiplication.

4. The set of maps $T : \mathbb{R}^3 \to \mathbb{R}^3$ such that $\|T(x) - T(y)\| = \|x - y\|$ for all $x, y \in \mathbb{R}^3$, under composition. (For a vector $v = (v_1, v_2, v_3) \in \mathbb{R}^3$, such as $x - y$ or $T(x) - T(y)$, $\|v\|$ denotes its Euclidean length, namely $\|v\| = \sqrt{v_1^2 + v_2^2 + v_3^2}$.) Distance-preserving maps such as these are called *isometries*. You may use, without proof, the fact that isometries of $\mathbb{R}^n$ are always onto (aka surjective).

Problem 5. (Cross-cancellation implies commutativity, Gallian 2.14) Let G be a group with the following property: Whenever a, b and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian.