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

Problem Set 1

Assigned: Wed. Sept. 9, 2009 Due: Wed. Sept. 23, 2009 (1:10 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`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details.
- If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.ps`). Name your files `PS1-yourlastname`.
- AM206 students should do the problems marked [AM206-X], and need not do the ones marked [AM106-X]. AM106 students need not do the problems marked [AM206-X], but may do so in place of the corresponding [AM106-X] problem (but not [AM106-Y] for Y $\neq X$) if desired.

Problem 1. (Solving Equations via Euclid)

1. **[AM106-A]** Use the Extended Euclidean Algorithm to compute $\gcd(11312, 600)$ and express it as an integer linear combination of 11312 and 600. Show your work.
2. **[AM106-A]** Find an integer solution to the equation $11312x + 600y = 40$.
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.

Problem 2. (Fibonacci numbers and the Euclidean Algorithm) The Fibonacci numbers $F_0, F_1, \ldots$ are defined inductively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$. Thus the sequence (starting at F_0) is $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$.

1. Prove by induction that for $n \geq 2$, $F_n \geq \varphi^{n-2}$, where $\varphi = (1 + \sqrt{5})/2$ is the golden ratio.
2. Prove by induction that if the Euclidean Algorithm makes $k \geq 1$ divisions when computing $\gcd(x, y)$, where $x > y \geq 1$, then $x \geq F_{k+2}$. Deduce that the number of divisions used when computing the gcd of two n-bit numbers is at most $(\log_\varphi 2) \cdot n = 1.44n$.

Problem 3. (Equivalence of induction axioms, Gallian 0.29) Prove that the Well-ordering Principle implies (Standard) Induction.

Problem 4. (Asymptotic Notation) True or False? Briefly justify your answers (e.g. in one sentence per part).

1. $2n = O(n)$
2. $n^2 = O(n)$
3. $n^2 = \Omega(n)$
4. $n^2 = O(n \log^2 n)$
5. $n \log n = O(n^2)$
6. $3^n = 2^{O(n)}$
7. $3^n = \Theta(2^n)$
8. $2^{2^n} = O(2^{2^n})$

Problem 5. (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 $x^y \bmod z$. (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 6. (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 $2n$-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 7. (Equivalence relations) Which of the following are equivalence relations? If it is an equivalence relation, describe the equivalence classes. If it is not, which property fail?

1. Set: $\mathbb{Z}$. Relation:
   $a \sim b$ if a, b are coprime (i.e $gcd(a, b) = 1$).
2. Set: $\mathbb{Z}$. Relation:
   $a \sim b$ if $a | b$.
3. Set: $\mathbb{R}$. Relation:
   $a \sim b$ if $a - b$ is an integer.

Problem 8. (Groups) Which of the following are groups? For those that are finite groups write a Cayley table. Briefly justify your answer.

1. $\{0, 2, 4, 6, 8\}$ with addition mod 9.
2. $\{1, 3, 4, 12\}$ with multiplication mod 13.
3. The powers of 2: $\{1, 2, 4, 8, \ldots\}$ under multiplication.
4. Set of affine-linear functions $f(x) = ax + b$, with $a \in \mathbb{Q} - \{0\}$ and $b \in \mathbb{Q}$. Operation: composition.
5. $O_n(\mathbb{R})$ = set of $n \times n$ real matrices M such that $MM^t = I$, where M^t is the transpose of M (whose (i, j) entry is the (j, i) entry of M). Operation: matrix multiplication. (Students who haven't had linear algebra should read example 9 in Gallian and do the $n = 2$ case).