Computer Science CSC478/2412 Spring 1997
St. George Campus University of Toronto

Homework Assignment #2
Due: Tuesday, 11 February 1997
Mark: 15%

1. Problem 5, page 106 of the textbook. Put $f(x, y)$ and $g(x, y)$ into the four normal forms discussed in Section 3.5 of the textbook, that is, *factored/factored, factored/expanded, expanded/factored, expanded/expanded*, with numerator and denominator relatively prime in each case.

2. Problem 6, page 107 of the textbook.

3. Prove that the extended Euclidean algorithm for $f \geq g \geq 0$ over $\mathbf{Z}$ the s_i and t_i alternate in sign, that is, s_{2i} and t_{2i-1} are positive, and s_{2i+1} and t_{2i} are negative, for all $i \geq 1$. Prove that $|s_i|$ and $|t_i|$ are monotonically increasing for $i \geq 1$.

4. This exercise gives the cost of the EEA over the integers. Let us represent the integers in binary with leading bit equal to 1. The *binary length* $\lambda(a)$ of a positive number a is the number of bits in the binary representation of a, that is, $\lambda(a) = \lfloor \log a \rfloor + 1$.

a. Show that the bound $\ell \leq |g| + 1$ is exponential in the input size $\lambda(f) + \lambda(g)$.

b. Prove the polynomial upper bound $\ell \leq 1 + 2 \log f$. Hint: first show that $a_{i-1} \geq 2a_{i+1}$ for $1 \leq i \leq \ell$; then, consider the product on both sides of the previous inequality for $1 \leq i < \ell$; finally, conclude that $2^{\ell-1} < a_0^2$. [In fact, it is possible to prove a better upper bound for ℓ: $1.441 \log_2 f + O(1)$ using Fibonacci numbers. The average length is also known: $0.584 \log_2 f$ (see Knuth 1981; §4.5.3).]

c. Consider the number of bit operations as the cost measure. This concept can be formally defined as the number of steps in a Turing machine or the number of gates of a Boolean circuit implementing the algorithm (for instance, see Aho, Hopcroft and Ullman, Ch. 1). Give the cost of one division step using the "school" division. The cost should be analogous to the one proven in class for division of polynomials with the only difference of possible carries during subtractions.

d. Prove the following theorem.

Theorem. The EEA for integers of binary length at most n bits can be performed with $O(n^2)$ bit operations.

Hint: use the same proof as the one for polynomials.

5. This exercise shows an application of the Chinese remainder algorithm.

a. Develop an algorithm for solving systems of linear equations with integer and rational coefficients by using the Chinese remainder algorithm. Implement your algorithm in MAPLE. You are allowed to use the MAPLE procedure `Solve` mod p, but not `Solve` over the integers or rational numbers. Test your algorithm with the examples in pages 151 and 404 of the textbook.

b. Apply your algorithm to solve the following linear equations for $n = 4, 5, 6, 7$:

$$\sum_{i=1}^{n} \frac{1}{i+j-1} x_i = j, \qquad j = 1, \ldots, n.$$

c. Use your algorithm and interpolations to solve:

$$\begin{aligned} ax + ay - z &= 1 \\ a^2x - y + z &= a \\ -x + y + az &= a^2 \end{aligned}$$

where a is a parameter.

6. Problem 14, page 332 of the textbook.

References

A. V. AHO AND J. E. HOPCROFT AND J. D. ULLMAN, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading MA, 1974.

K. O. GEDDES AND S. R. CZAPOR AND G. LABAHN, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, Boston, 1992.

D.E. KNUTH, *The Art of Computer Programming, vol.2: Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading MA, 1981.