# MACM 401/MATH 701, MATH 819/CMPT 881
# Assignment 1, Spring 2008.

Michael Monagan

This assignment is to be handed in by Thursday January 22nd at the beginning of class.
Late penalty: $-20\%$ for up to 24 hours late. Zero after that.
For problems involving Maple calculations and Maple programming, you should submit a printout of a Maple worksheet of your Maple session.

## Question 1 (10 marks): Karatsuba's Algorithm

(a) By hand, calculate $5432 \times 3829$ using Karatsuba's algorithm. You will need to do three recursive multiplications involving two digit integers. Do the first one, $54 \times 38$, using Karatsuba's algorithm. Do the others using the classical algorithm to save work.

(b) Let $T(n)$ be the time it takes to multiply two $n$ digit integers using Karatsuba's algorithm. For simplicity, assume $n = 2^k$. For $n > 1$, we have $T(n) \leq 3T(n/2) + cn$ for some constant $c > 0$ and $T(1) = d$ for some constant $d > 0$. First show that $n^{\log_2 3} = 3^k$. Now solve the recurrence relation and show that $T(n) \in O(n^{\log_2 3})$ or show that $T(n) \in O(3^k)$. Show your working.

## Question 2 (10 marks): Integer GCD Algorithms

(a) Implement the binary GCD algorithm in Maple as the Maple procedure named BINGCD. Use the Maple functions `irem` and `iquo` for dividing by 2. Test your procedure on the integers $a = 16 \times 3 \times 101$ and $b = 8 \times 3 \times 203$. Print out the sequence of odd pairs of integers $(a, b)$ with $a \geq b$ that appear in the algorithm.

(b) Time Maple's `igcd(a,b);` command on random pairs of integers $(a, b)$ of suitable lengths to experimentally determine the time complexity of the algorithm Maple is using. For example, integers of lengths $n = 20000$, 40000, 80000, and 160000 decimal digits.

## Question 3 (20 marks): Integral Domains

Let $S$ be the subset of the complex numbers $\mathbb{C}$ defined by

$$S = \{a + b\sqrt{-5} : \ a, b \in \mathbb{Z}\}$$

where addition in $S$ is defined by $(a+b\sqrt{-5})+(c+d\sqrt{-5}) = (a+c)+(b+d)\sqrt{-5}$ and multiplication is defined by $(a + b\sqrt{-5}) \times (c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$.

(a) Assume $S$ is a commutative ring. Show that $S$ has no zero divisors and hence conclude that $S$ is an integral domain.

(b) Show that the only units in $S$ are $+1$ and $-1$.

(c) Show that $S$ is not a unique factorization domain. Hint: show that the element 21 has two different factorizations into irreducibles. Hint: $1 - 2\sqrt{-5}$ is an irreducible factor of 21. Note: you must show that your factors are irreducible.

(d) Show that the elements $a = 147$ and $b = 21 - 42\sqrt{-5}$ in $S$ have no greatest common divisor. Hint: first show that 21 and $7 - 14\sqrt{-5}$ are both common divisors of $a$ and $b$.

## Question 4 (20 marks): Euclidean Domains

Let $G$ be the subset of the complex numbers $\mathbb{C}$ defined by $G = \{x + y\,i : x, y \in \mathbb{Z},\ i = \sqrt{-1}\}$. $G$ is called the set of Gaussian integers and is usually denoted by $\mathbb{Z}[i]$.

(a) Why is $G$ an integral domain? What are the units in $G$?

Let $a, b \in G$. In order to define the remainder of $a$ divided by $b$ we need a measure $v : G \to \mathbb{N}$ for the size of a non-zero Gaussian integer. We cannot use $v(x + iy) = |x + iy| = \sqrt{x^2 + y^2}$ the the length of the complex number $x + iy$ because it is not an integer valued function. We will instead use the norm $N(x + iy) = x^2 + y^2$ for $v(x + iy)$ which has the following useful properties.

(b) Show that for $a, b \in G$, $N(ab) = N(a)N(b)$ and $N(ab) \geq N(a)$.

(c) Now, given $a, b \in G$, where $b \neq 0$, find a definition for the quotient $q$ and remainder $r$ satisfying $a = b\,q + r$ with $r = 0$ or $v(r) < v(b)$ where $v(x + iy) = x^2 + y^2$. Using your definition calculate the quotient and remainder of $a = 63 + 10i$ divided by $b = 7 + 43i$.

Hint: consider the real and imaginary parts of the complex number $a/b$ and consider how to choose the quotient of $a$ divided $b$. Note, you must prove that your definition for the remainder $r$ satisfies $r = 0$ or $v(r) < v(b)$. The multiplicative property $N(ab) = N(a)N(b)$ will help you. Now since part (b) implies $v(ab) \geq v(b)$ for non-zero $a, b \in G$, this establishes that $G$ is a Euclidean domain.

(d) Finally write a Maple program REM that computes the remainder $r$ of $a$ divided $b$ using your definition from part (c). Now compute the gcd of $a = 63 + 10i$ and $b = 7 + 43i$ using the Euclidean algorithm and your program. You should get $2 + 3i$ up to a unit. Note, in Maple `I` is the symbol used for the complex number $i$ and you can use the `Re` and `Im` commands to pick off the real and imaginary parts of a complex number. Also, the `round` function may be useful. For example

```
> a := 2+5/3*I;
                                   a := 2 + 5/3 I

> Re(a);
                                        2

> Im(a);
                                       5/3

> round(a);
                                      2 + 2 I
```

## Question 5 (10 marks): The Extended Euclidean Algorithm

Reference: Algorithm 2.2 in the Geddes text.
Given $a, b \in \mathbb{Z}$, the extended Euclidean algorithm solves $sa + tb = g$ for $s, t \in \mathbb{Z}$ and $g = \gcd(a, b)$. More generally, for $i = 0, 1, ..., n, n + 1$ it computes integers $(r_i, s_i, t_i)$ where $r_0 = a, r_1 = b$.

(a) For $m = 99$, $u = 28$ execute the extended Euclidean algorithm with $r_0 = m$ and $r_1 = u$ by hand. Use the tabular method presented in class that shows the values for $r_i, s_i, t_i, q_i$. Hence determine the inverse of $u$ modulo $m$.

(b) Repeat part (a) but this time use the symmetric remainder, that is, when dividing $a$ by $b$ choose the quotient $q$ and remainder $r$ such that $a = bq + r$ and $-\lceil |b/2| \rceil < r < \lfloor |b/2| \rfloor$ instead of $0 \leq r < b$.

**Question 6 (10 marks): Math 819 students only**

Suppose we call the extended Euclidean algorithm with inputs $a \geq b > 0$. Thus $r_0 = a, r_1 = b$ and $r_n = g$ where $g = \gcd(a, b)$. Prove the following properties about the integers $t_0, t_1, ..., t_n, t_{n+1}$ that appear in the extended Euclidean algorithm (assuming the positive remainder is used).

(i) $|t_{i-1}| < |t_i|$ for $i = 3, ..., n + 1$.

(ii) $r_i\, t_{i-1} - r_{i-1}\, t_i = (-1)^i\, a$ for $i = 1, ..., n + 1$.

(iii) $t_{n+1} = (-1)^n a/g$. Hint: put $i = n + 1$ into (ii).

Since the $t_i$ are increasing in magnitude from (i), then (iii) implies $|t_n| < a/g$. Suppose we call the extended Euclidean algorithm with input $a = m$ and $b = u$ to compute the inverse of $u$ modulo $m$. If $g = 1$, then we have $-m < t_n < m$ and hence it suffices to add $m$ to $t_n$ if $t_n < 0$.