MACM 401/MATH 801
Assignment 1, Spring 2019.

Michael Monagan

This assignment is to be handed in by 4pm Monday January 21st.
Hand in to Dropoff box 1A outside AQ 4100.
Late penalty: −20% for up to 48 hours late. Zero after that.
For problems involving Maple calculations and Maple programming, please submit a printout of a Maple worksheet.

Question 1 (15 marks): Karatsuba's Algorithm

Reference: Algorithm 4.2 in the Geddes text.

(a) By hand, calculate 5432×3829 using Karatsuba's algorithm. You will need to do three multiplications involving two digit integers. Do the first one, 54×38, using Karatsuba's algorithm (recursively). Do the other two using any method.

(b) Let $T(n)$ be the time it takes to multiply two n digit integers using Karatsuba's algorithm. We will assume (for simplicity) that $n = 2^k$ for some $k > 0$. Then 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 $3^k = n^{\log_2 3}$. Now solve the recurrence relation and show that $T(n) = (2c + d)n^{\log_2 3} - 2cn$ thus concluding that $T(n) \in O(n^{\log_2 3}) = O(n^{1.585})$. Show your working.

(c) Show that $T(2n)/T(n) \sim 3$, that is, if we double the length of the integers then the time for Karatsuba's algorithm increases by a factor of 3 (asymptotically).

Question 2 (15 marks): GCD Algorithms

(a) Implement the binary GCD algorithm in Maple as the Maple procedure named BINGCD to compute the GCD of two positive integers a and b. Use the Maple functions `irem(a,b)` and `iquo(a,b)` for dividing by 2.

Your Maple code will have a main loop in it. Each time round the loop please print out current values of (a, b) using the command

```
printf("a=%d  b=%d\n",a,b);
```

so that you and I can see the algorithm working. Test your procedure on the integers $a = 16 \times 3 \times 101$ and $b = 8 \times 3 \times 203$.

(b) I think Maple's command `GCD(A,B) mod p;` uses the Euclidean algorithm to compute the GCD of two polynomials $A(x)$ and $B(x)$ in the ring $\mathbb{Z}_p[x]$. [We will show later that for two polynomials $A(x)$ and $B(x)$ of degree d, the Euclidean algorithm does $O(d^2)$ arithmetic operations in $\mathbb{Z}_p$.] Let's verify if this could true by timing Maple's `Gcd(A,B) mod p;` command and seeing if the times are quadratic in the degree d. Execute the following code in Maple and test to see if the times you get are quadratic in d. Justify your answer. Hint: if $T(d)$ is the time and $T(d)$ is quadratic in d, what should $T(2d)/T(d)$ approach when d large?

```
d := 1000;
p := prevprime(2^30);
for i to 7 do
    A := Randpoly(d,x) mod p;
    B := Randpoly(d,x) mod p;
    st := time();
    G := Gcd(A,B) mod p;
    tt := time()-st;
    printf("deg=%d  G=%a  time=%7.3fsecs \n",d,G,tt);
    d := 2*d;
od:
```

Question 3 (20 marks): The Gaussian Integers

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 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 $v(x + iy)$.

(b) Show that for $a, b \in G$, $N(ab) = N(a)N(b)$.
Show that for $a, b \in G$ with $b \neq 0$, $N(ab) \geq N(a)$.

(c) Let $a, b \in G$ with $b \neq 0$. Find a definition for the quotient q and remainder r satisfying $a = b\,q + r$ with $r = 0$ or $v(r) < v(b)$ where $v(x + iy) = N(x + iy) = x^2 + y^2$. 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 procedure `REM` such that `REM(a,b)` 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 `REM` procedure. You should get $2 + 3i$ up to multiplication by a unit. Also, test your procedure on $a = 330$ and $b = -260$.

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 4 (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 $r_0 = a, r_1 = b$ satisfying $s_i a + t_i b = r_i$ for $0 \le i \le n+1$.

(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 are integers satisfying $a = bq + r$ and $-|b/2| \le r < |b/2|$ instead of $0 \le r < b$.

Question 5 (10 marks): MATH 701 and MATH 801 students only

Suppose we call the extended Euclidean algorithm with integers $a \ge b > 0$. 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 $-m < t_n < m$ by (iii) and hence to compute u in the positive range we have

if $t_n < 0$ **then** $u := t_n + m$ **else** $u := t_n$ **fi**;