MACM 401/MATH 801/CMPT 981
Assignment 1, Spring 2021.

Michael Monagan

This assignment is to be handed in by 11pm Monday January 25th.
Do each question separately on paper or in a Maple worksheet or on a tablet.

If you use paper, take a photo of your work with your phone or scan it. If you use a tablet, export your work to a .pdf file. For problems involving Maple calculations and Maple programming, export the Maple worksheet to a .pdf file.

You will upload your assignment to crowdmark. You will be sent an Email with a link from crowdmark. You will upload your solution to each question to a separate crowdmark box.

Late penalty: -20% for up to 24 hours late. Zero after that.

Question 1 (15 marks): Karatsuba's Algorithm

Reference: Algorithm 4.2 in the Geddes text.

(a) By hand, calculate 8484×3829 using Karatsuba's algorithm. You will need to do three multiplications involving two digit integers. However, one of the multiplications will be trivial. For the other two, 84×38 and 84×29, use Karatsuba's algorithm recursively.

(b) Let $T(n)$ be the time it takes to multiply two n digit integers using Karatsuba's algorithm. 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 (for large n).

Question 2 (10 marks): Using Maple as a Calculator

(a) Use Maple to calculate and simplify the following sums

$$\sum_{k=1}^{n} k^2 \ , \quad \sum_{k=1}^{n} k^3 \ , \quad \sum_{k=1}^{n} \binom{n}{k} \quad \text{and} \quad \sum_{k=1}^{n} k \binom{n}{k}.$$

The geometric sums

$$\sum_{k=0}^{\infty} q^k \quad \text{and} \quad \sum_{k=0}^{\infty} (k+1) q^k$$

converge for $|q| < 1$. To evaluate these sums in Maple, use the following functionality in Maple to tell Maple that $|q| < 1$.

```
> sum( ... ) assuming q>-1 and q<1;
```

(b) Use Maple's `rsolve` command to solve the following recurrences.

$$a(n) = 2a(n-1) + 1 \text{ with } a(1) = 1 \tag{1}$$

$$f(n) = f(n-1) + f(n-2) \text{ with } f(0) = 0, f(1) = 1 \tag{2}$$

$$T(n) = 4T(n/2) + cn \text{ with } T(1) = d. \tag{3}$$

See the Maple help page for `rsolve` for examples. For the Fibonacci recurrence in (2), you will get a formula

$$-\frac{\sqrt{5}\left(-\frac{\sqrt{5}}{2}+\frac{1}{2}\right)^n}{5} + \frac{\sqrt{5}\left(\frac{\sqrt{5}}{2}+\frac{1}{2}\right)^n}{5} \tag{4}$$

that does not look like it is integer valued. Evaluate (4) at $n = 4$ and check that the result simplifies to 3.

Question 3 (10 marks): The binary GCD algorithm

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 $a = 16\times3\times101$ and $b = 8 \times 3 \times 203$.

Question 4 (25 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) (6 marks) Why is G an integral domain? What are the units in G?

Let $a, b \in G$ with $b \neq 0$. In order to define the remainder of $a \div b$ we need a measure $v : G \to \mathbb{N}$ for the size of a non-zero Gaussian integer. We cannot use $v(x + iy) = |x + iy| = \sqrt{x^2 + y^2}$ because it is not an integer valued function. Use $N(x + iy) = x^2 + y^2$ for $v(x + iy)$.

(b) (4 marks) 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) (9 marks) 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 $v(x + iy) = N(x + iy) = x^2 + y^2$. Note, you must prove that your choice for q and r satisfies $r = 0$ or $v(r) < v(b)$. Then since part (b) shows $v(ab) \geq v(b)$ this establishes that G is a Euclidean domain. Using your definition calculate the quotient and remainder of $a = 63 + 10i$ divided by $b = 7 + 43i$.

Hint: if $a = bq + r$ and $b \neq 0$ then $a/b - q = r/b$. Try choosing q so that $|a/b - q|$ is small.

(d) (6 marks) 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 5 (15 marks): Algorithm Complexity

(a) For a constant $c > 0$ and function $f : \mathbb{N} \to \mathbb{R}$ show that $O(cf(n)) = O(f(n))$.
It is sufficient to show (i) $cf(n) \in O(f(n))$ and (ii) $f(n) \in O(cf(n))$.

(b) Show that $O(\log_a n) = O(\log_b n)$. The easiest way to do this is to convert both logarithms to base e using $\log_a n = \frac{\log_e n}{\log_e a} = \frac{\ln n}{\ln a}$.

(c) Let $\mathbb{Z}_p$ denote the field of integers modulo p a prime. 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 see if this could true by timing Maple's `Gcd(A,B) mod p;` command to see if the times are quadratic in 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:
```