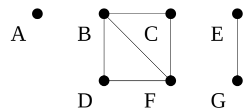
last name ______________________ first names ______________________ ID ______________________

16oct2014 45min 30 marks no devices

1. [7 marks]



The graph has $n = 7$, $m = 6$, and $t = 3$ components. The output is combined preorder/postorder, followed by n, $2m$, t:

`A A B C F D D F C B E G G E 7 [12] 3`

2. [4 marks] For integers $1 < j < n$, Euclid's `gcd(n,j)` performs $O(\log n)$ integer divisions, each on numbers with $O(\log n)$ bits. One such division takes $O(\ (\log n)^2\ )$ time, so total run time is $O(\ (\log n)^3\ )$.

3. [4 marks]

```
                 1  1  0  1  1
               --------------
            \/ 10 11 01 11 01
1                1
                 ----
                 1 11
101              1 01
                 -------
                 0 10 01
1100                   0
                 ----------
                   10 01 11
11001               1 10 01
                   -----------
                      11 10 01
110101                11 01 01
                      --------
                          1 00
```

- root 1 1 0 1 1
- remainder 1 0 0

last name ______________ first names ______________ ID ______________

4. [6 marks]

```
( 25 0 ) 0
( 25 1 ) 25
( 25 3 ) 75
( 25 6 ) 150
( 25 12 ) 300
( 25 25 ) 625
```

Let $t = 9801$. Assume that, for all integers y with $0 \leq y \leq t$, `rmult(x,y)` returns x times y.

Claim. `rmult(x,9802)` returns x times 9802.

Proof. 9802 is even, so `rmult(x,9802)` returns `2 times rmult(x,4901)`. Also, `4901` is less than `9801`,

so by our assumption `rmult(x,4901)` returns `x times 4901` .

So `rmult(x,9802)` returns

`2 * rmult(x,4901) =`

`2 * x * 4901 =`

`x * 9802.  QED.`

5. [3 marks] Consider the MillerRabin test to see whether 561 is prime. A number a is picked randomly from this set of integers: {2,3,. . . ,559}.

Next, a is raised to these powers (mod 561):

35 70 140 280 560 .

Assume that $a^{560} = 1$ (mod 561). Then, by the Euclid — or non-trivial root of unity — test,

561 is composite if $a^{280} \neq \pm 1$ (mod 561), or

$a^{280} = 1$ and $a^{140} \neq \pm 1$, or

$a^{140} = 1$ and $a^{70} \neq \pm 1$, or

$a^{70} = 1$ and $a^{35} \neq \pm 1$.

6. [3 marks] In each case, give the simplest Θ expression for $T(n)$. Hint: master theorem: compare a and b^d.

- $T(n) = 9T(n/3) + \Theta(n^2)$

  a 9 b 3 d 2 $a = b^d$

  $\Theta(n^2 \log n)$

- $T(n) = 6T(n/2) + \Theta(n^2)$

  a 6 b 2 d 2 $a > b^d$

  $\Theta(n^{\log_2 6})$

- $T(n) = \Theta(n^3) + 8T(n/4)$

  a 8 b 4 d 3 $a < b^d$

  $\Theta(n^3)$

7. [3 marks]

```
Arithmetic is mod 7. For fast exp'n,
compute these powers of 5: 1 3 6 12 24.

5^1 = 5
5^3 = (5^1)^2 * 5
    = 5^2 * 5 = 25 * 5
    = (25 mod 7) * 5 = 4 * 5
    = 20 = 6 = -1
5^6 = (5^3)^2 = (-1)^2 = 1
5^12 = (5^6)^2 = 1^2 = 1
5^24 = (5^12)^2 = 1^2 = 1
```