CS 3511 - Spring 2009
Homework 1
Due: February 11

The honors students must do this homework in addition to the standard (3510) homework. Hopefully these will be a little more challenging and interesting. Non-honors students are also encourage to do these problems! **The "extra-credit" applies to everyone!** Again, you need to work alone and without calculators.

1. Compute $x^y \bmod 23$ for $x = 13$ and $y = 37^{192}$.

   First note that by Fermat's little theorem, for any prime p and a such that $a \neq 0 \pmod{p}$,

   $$a^{p-1} \equiv 1 \pmod{p}$$

   so it follows that

   $$a^y \equiv a^{y \pmod{p-1}} \pmod{p}.$$

   Therefore we should start by calculating $37^{192} \pmod{22}$.

   Now recall that if p and q are prime and a is relatively prime to pq, then

   $$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

   We use this with $p = 2$ and $q = 11$, so $(p-1)(q-1) = 10$. Therefore,

   $$37^{10} \equiv 1 \pmod{22}$$

   which implies

   $$37^{192} \equiv 37^2 * (37^{10})^1 9 \equiv 37^2 \equiv 1369 \equiv 5 \pmod{22}.$$

   Putting these together, we find that when $x = 13$ and $y = 37^{192}$

   $$x^y \bmod 23 \equiv 13^5 \pmod{23}.$$

   We find this value by repeated squaring:

   $$13^1 \equiv 13 \pmod{23}.$$

$$13^2 \equiv 169 \equiv 8 \pmod{23}.$$
$$13^4 \equiv 64 \equiv 18 \pmod{23}.$$

Putting this together, we have

$$\begin{aligned} 13^5 &= 13^4 * 13 \pmod{23} \\ &\equiv 18 * 13 \pmod{23} \\ &\equiv 234 \equiv 4 \pmod{23}. \end{aligned}$$

Therefore $x^y = 4 \bmod 23$ for $x = 13$ and $y = 37^{192}$.

2. Prove the Master Theorem.

   (a) First, argue that if at each level a problem of size x is broken into a problems of size x/b and if it takes x^d work to recombine the results from the recusion, then:
      i. The top level of the tree requires n^d work.
      ii. The bottom level of the tree has $a^{log_b n} = n^{log_b a}$ leaves, and requires that much total work.
      iii. Figure out how much work each intermediate level of the tree requires, and write the *t*otal amount of work (on all levels of the tree as a summation.

   (b) Now evaluate your summation in three cases: (a) $d = \log_b a$ (b) $d < \log_b a$, (c) $d > \log_b a$.

   Hint: For parts (b) and (c), it will be useful for you to verify and use the following identity for appropriate choices of x, r and k:

$$x + xr + xr^2 + \ldots + xr^k = \frac{xr^{k+1} - 1}{r - 1}$$

   Proof. Draw a tree recursion for $T(n)$: $f(n)$ is the root and it has a children each of which is a recursion tree for $T(n/b)$. That is, a recusion tree is a complete a-ary tree where each node at depth i has the value $a^i f(n/b^i)$. The leaves of the tree contains the base cases of the recusion. Since we are looking at asymptotic bounds, we can assume without lost of generality that T(1) = f(1). Assuming each level of the tree is full, we have,

$$T(n) = f(n) + af(n/b) + a^2 f(n/b^2) + \ldots + a^L f(n/b^L)$$

   where L is the depth of the recursion tree
   .
   $L = \log_b n$ and since $f(1) = \Theta(1)$,

$$a^L f(n/b^L) = \theta(a^{\log_b n}) = \theta(n^{\log_b a})$$

1) f(n) is a constant factor larger than $a * f(n/b)$ then $T(n)$ is a geometric series with the largest term $f(n)$. Hence $T(n) = \theta(f(n))$.

2)If $f(n)$ is a constant factor smaller than a*f(n/b) then $T(n)$ is a geometric series with the largest term $a^L f(n/b^L) = \theta(n^{\log_b a})$.

3) If $a * f(n/b) = f(n)$ then there are $L+1$ levels each level summing to $f(n)$ and hence $\theta(f(n)log_b n)$. □

3. **Extra Credit:** Seven prisoners in the land of Mathtopia are presented with a one-time chance to gain their freedom, but if they fail then they will all killed. At dawn, an integer between 1 and 7 will be written on each of their foreheads. Each sees the numbers on the other prisoners' heads, but cannot see his own. They simultaneously have to guess the number on their own head, and no communication between them prior to this is allowed. If even one person gusses correctly, then they will all be saved. However, if they are all incorrect, then ... well, you get the idea. Devise a strategy that will ensure their survival, no matter what numbers are placed on their heads!!

   First notice that if anyone knew the sum of all the seven numbers mod 7, then they would be able to deduce the number on their head. For example, if the sum of the seven numbers is known to be 4 mod 7, and if I see six numbers that sum to 6 mod 7, then I know that I have a 5 on my head.

   Now each person simply picks a different guess for what the sum is mod 7 !! Whoever guessed the right value can correctly deduce the number on his forehead, and exactly one of them is going to guess correctly. Therefore the prisoners will be saved.