Quiz 1 Solutions
CS3510 (and 3511), Algorithms,
February 13, 2009

1. **Problem 1**. [20 points]

   (a) What is $3^{65} \bmod 21$?

   Since 21 is not prime, we cannot apply Fermat's little theorem here. So we use the modular exponentiation algorithm described by the book.

   We start with $3^2 \bmod 21$ and build up to $3^{64} \bmod 21$.

   $$3^2 \bmod 21 = 9 \bmod 21$$

   We square the result to find $3^4 \bmod 21$ and so on.

   $$3^4 \bmod 21 = (9 \bmod 21)^2 = 81 \bmod 21 = 18 \bmod 21$$

   $$\begin{aligned} 3^8 \bmod 21 = (18 \bmod 21)^2 = (9{*}2 \bmod 21)^2 = (2 \bmod 21)^2{*}(9 \bmod 21)^2 \\ = (4 \bmod 21)(18 \bmod 21) = 72 \bmod 21 \\ = 9 \bmod 21 \end{aligned}$$

   $$3^{16} \bmod 21 = (9 \bmod 21)^2 = 18 \bmod 21, \text{ From } \ 3^4 \bmod 21$$

   $$3^{32} \bmod 21 = (18 \bmod 21)^2 = 9 \bmod 21, \text{ From } 3^8 \bmod 21$$

   $$3^{64} \bmod 21 = (9 \bmod 21)^2 = 18 \bmod 21\ , \text{ From } \ 3^4 \bmod 21$$

Now that we have $3^{65} \bmod 21$, we can solve the original problem.

$$3^{65} \bmod 21 = 3 * 3^{64} \bmod 21 = (3 \bmod 21)(3^{64} \bmod 21)$$

$$= (3 \bmod 21)(18 \bmod 21) = 54 \bmod 21 = 12 \bmod 21$$

(b) What is $25^{462} \bmod 11$?

Since 11 is prime, we can use Fermat's little theorem, which states that $a^{p-1} \equiv 1 \bmod p$. So we want to exploit the fact that $a^{10} \equiv 1 \bmod 11$.

$$25^{462} \bmod 11 = 25^{46*10} * 25^2 \bmod 11$$

$$= (25^{46*10} \bmod 11)(25 \bmod 11)^2$$

$$= (25^{46} \bmod 11)^{10}(3 \bmod 11)^2$$

$$= (1^{10} \bmod 11)(9 \bmod 11)$$

$$= 9 \bmod 11$$

2. **Problem 2**. [25 points]
Suppose there are two alternatives for solving a problem using divide and conquer by dividing a problem of size n into subproblems of smaller size:

- If you solve 3 subproblems of size $n/2$, then the cost of combining the solutions of the subproblems to obtain a solution for the original problem is $\Theta(n^{5/2})$.
- If you solve 4 subproblems of size $n/2$, then the cost for combining the solutions is $\Theta(n^2)$.

Which alternative do you prefer and why?

The recurrence for the first algorithm is

$$T_1(n) = 3T_1(n/2) + \Theta(n^{5/2})$$

We can use the Master theorem to find the overall running time and since $5/2 > \log_2 3$, we are in case 1.

So $T_1(n) = O(n^{5/2})$.

The recurrence for the second algorithm is

$$T_2(n) = 4T_2(n/2) + \Theta(n^2)$$

We can use the Master theorem to find the overall running time and since $2 = \log_2 4$, we are in case 2.

So $T_2(n) = O(n^2 \log n)$.

The function $n^{5/2}$ grows faster than $n^2 \log n$ as n approaches infinity. So the second approach is preferred and more efficient.

3. **Problem 3**. [25 points]
   True or false? If true, give a (short) proof. If false, give a counterexample.

   1. 1 has an inverse mod n for every integer $n > 1$.
      This statement is true. If 1 has an inverse mod n, then there exists an x such that $1x \equiv 1 \bmod n$. If n were 1, then for any value of x, $x \bmod n$ would be 0 and so no inverse would exist.

      Back to the original prolem, $x \bmod n = 1 \bmod n$. If $x = n + 1$ then $n + 1 \bmod n = 1 \bmod n$. Therefore $n + 1 \equiv 1 \bmod n$ and $n + 1$ is an inverse mod n for every $n > 1$.
   2. If p is a prime, then p has an inverse mod n for every integer $n > 1$.
      This statement is false. If $n = p$, then $px \bmod p = 0$ and no inverse exists.
   3. If $ax \equiv ay \bmod n$, then $x \equiv y \bmod n$.
      This statement is false.

      $$ax \bmod n - ay \bmod n = 0$$

      $$(a \bmod n)(x \bmod n) - (a \bmod n)(y \bmod n) = 0$$

      $$(a \bmod n)(x \bmod n - y \bmod n) = 0$$

      Either $a \bmod n = 0$ or $x \bmod n = y \bmod n$. If $a \bmod n = 0$, then it is not necessarily the case that $x \equiv y \bmod n$.

4. **Problem 4**. [30 points]
   For primes $p = 13$, $q = 29$, in the RSA cryptosystem:

1. Specify a valid public key.

   We should choose a value for e such that it is relatively prime to $(p-1)(q-1) = 366$. The values 2, 3, 4 are not relatively prime to 336 so we choose 5. So our public key is (377, 5).

2. What is a valid private key?

   To find a valid private key, d, we use the extended gcd to find x and y such that $e * x + (p-1)(q-1)y = 1$. Note that x is d, the inverse of e mod $(p-1)(q-1)$.

$$336 = 67 * 5 + 1$$

$$5 = 5 * 1 + 0$$

   So gcd(5, 336) = 1, which is what we would expect from relatively prime numbers. Now we run the extended Euclidean algorithm.

$$\begin{aligned} 1 &= 1 - 0 \\ &= 6 * 1 - 5 \\ &= 6(336 - 67 * 5) - 5 \\ &= 6 * 336 - 403 * 5 \end{aligned}$$

   So $d = -403$.

   Are there other choices for the private key?

   Yes, d can be $-403 + 336 * k$, where k is any integer. Additionally, the private key would be different if for a different choice of e.

3. If Alice wants to send the message $m = 3$, what would be the encrypted message she would send under the RSA protocol?

   3^5 mod 377 = 243 mod 377

   Is this encrypted message secure?

   No, this message is not secure because the values for p and q are too small, which result in a value for N that is easily factored.