Zheng Ma *March 1, 2005*

Solutions to Problem Set 3

Note: Each question counts 10 points.

Problem 6: Chinese remainder theorem

Solve the following system of equations for x:

$$x \equiv 1 \pmod{5}$$
$$x \equiv 4 \pmod{11}$$
$$x \equiv 3 \pmod{17}$$

Solution: Because $n_1 = 5$, $n_2 = 11$ and $n_3 = 17$ are pairwise relatively prime positive integers, we can apply Chinese Remainder Theorem directly, where $a_1 = 1$, $a_2 = 4$, and $a_3 = 3$:

$$n = \Pi_{i=1}^{3} n_i = 935$$
$$N_1 = n/n_1 = 187, M_1 \equiv N_1^{-1} \equiv 3 \pmod{n_1}$$
$$N_2 = n/n_2 = 85, M_2 \equiv N_2^{-1} \equiv 7 \pmod{n_2}$$
$$N_3 = n/n_3 = 55, M_3 \equiv N_3^{-1} \equiv 13 \pmod{n_3}$$
$$x = (\textstyle\sum_{i=1}^{3} a_i M_i N_i) \equiv 411 \pmod{n}.$$

This answer is easily verified by computing $411 \bmod n_i$ for $i = 1, 2, 3$.

Problem 7: Primitive roots

(a) Give a formula for the number of primitive roots of p when p is prime, and evaluate this formula for $p = 11$ and $p = 23$.

(b) Find all primitive roots of p, for $p = 11$ and $p = 23$. You may use a computer.

Solution:

(a) The number of primitive roots of prime p is $\phi(\phi(p))$. So $\phi(\phi(11)) = \phi(10) = 4$ and $\phi(\phi(23)) = \phi(22) = 10$.

(b) We can use the Lucas test to find all the primitive roots of p as in the following program:

```
#include <lnv3/lnv3.h>
#include <nttl/gcd.h>
#include <nttl/randomPrime.h>
#include <nttl/inverse.h>
#include <stdio.h>
main(int argc, char** argv){
        ln x, p,p_1,q;
        int i,prime=11;
        prime = ((argc > 1) ? atoi(argv[1]):prime);
```

```
            p = (ln) prime;
            p_1 = p -1;
            bool test;
            for(x=1 ; x < p; x++){
            test = true;
            for(i=2; i < p;i++){
             if(p_1 % i == 0){
                    q = p_1/i;
                    if(x.FastExp(q,p)== 1) {test=false;break;}
             }
            }
             if(test) cout<< x << " is a primitive root" <<endl;
            }
}
```

So, the primitive roots for 11 are $\{2, 6, 7, 8\}$. The primitive roots for 23 are $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$.

Problem 8: Square roots

Find all square roots of 1 modulo 77. Again, you may use the computer.

Solution: You can write a program to solve this. Here, we show how to find the square roots of 1 without using a computer. We notice that $n = p \times q = 7 \times 11$, and p and q are primes. So $a \in \mathrm{QR}_{77}$ has exactly four square roots in $\mathbf{Z}^*_{77}$. Let b is one of the square roots, i.e. $b^2 \equiv 1 \pmod{77}$. So $b^2 \equiv 1 \pmod 7$ and $b^2 \equiv 1 \pmod{11}$. So b must be a square root of 1 in both $\mathbf{Z}^*_7$ and $\mathbf{Z}^*_{11}$. Now we know that $\{(1, 1), (-1, -1), (1, -1), (-1, 1)\}$ are four such elements in $\mathbf{Z}^*_7 \times \mathbf{Z}^*_{11}$. These correspond to $\{1, 76, 43, 34\} \in \mathbf{Z}^*_{77}$ by the Chinese Remainder Theorem.