Practical No. 9

Aim: To implement Chinese Remainder Theorem to perform primality testing.

Theory:

The Chinese Remainder Theorem (which will be referred to as CRT in the rest of this article) was discovered by Chinese mathematician Sun Zi.

Formulation

Let $p=p_1 \cdot p_2 \cdots p_k$, where p_i are pairwise relatively prime. In addition to p_i, we are also given a set of congruence equations

$a \equiv a_1 (\bmod p_1)$
$a \equiv a_2 (\bmod p_2) \ldots$
$a \equiv a_k (\bmod p_k)$

where a_i are some given constants. The original form of CRT then states that the given set of congruence equations always has one and exactly one solution modulo p.

Corollary

A consequence of the CRT is that the equation

$x \equiv a (\bmod p)$

is equivalent to the system of equations

$x \equiv a_1 (\bmod p_1)$
...
$x \equiv a_k (\bmod p_k)$

(As above, assume that $p=p_1 p_2 \cdots p_k$ and p_i are pairwise relatively prime).

Garner's Algorithm

Another consequence of the CRT is that we can represent big numbers using an array of small integers. For example, let p be the product of the first 1000 primes. From calculations we can see that p has around 3000 digits.

Any number a less than p can be represented as an array $a_1,\ldots,a_k$, where $a_i \equiv a \pmod{p_i}$. But to do this we obviously need to know how to get back the number a from its representation. In this section, we discuss Garner's Algorithm, which can be used for this purpose. We seek a representation on the form

$$a = x_1 + x_2 \cdot p_1 + x_3 \cdot p_1 \cdot p_2 + \ldots + x_k \cdot p_1 \cdots p_{k-1}$$

which is called the mixed radix representation of a. Garner's algorithm computes the coefficients $x_1,\ldots,x_k$.

Let r_{ij} denote the inverse of p_i modulo p_j

$$r_{ij} = (p_i)^{-1} \pmod{p_j}$$

which can be found using the algorithm described in Modular Inverse. Substituting a from the mixed radix representation into the first congruence equation we obtain

$$a_1 \equiv x_1 \pmod{p_1}.$$

Substituting into the second equation yields

$$a_2 \equiv x_1 + x_2 p_1 \pmod{p_2}.$$

which can be rewritten by subtracting x_1 and dividing by p_1 to get

$$a_2 - x_1 \equiv x_2 p_1 \pmod{p_2}$$
$$(a_2 - x_1) r_{12} \equiv x_2 \pmod{p_2}$$
$$x_2 \equiv (a_2 - x_1) r_{12} \pmod{p_2}$$

Similarly we get that

$$x_3 \equiv ((a_3 - x_1) r_{13} - x_2) r_{23} \pmod{p_3}.$$

Conclusion: Chinese Remainder Theorem to perform primality testing is implemented successfully.

Viva Questions:

Q. 1 What is Concept of co-prime?

Q. 2 What is use of Chinese Remainder Theorem in Cryptography?

Q. 3 What is concept Chinese Remainder Theorem?