Coding and Cryptography Notes

Daniel da Silva

November 2016

1 Theorem and Algorithms

1.1 Euclids's Algorithm

1.1.1 Statement

To find the GCD of two numbers, say a and b $(b < a)$, do the following:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &. \\ &. \\ &. \end{aligned}$$

Since the remainder is decreasing with every step but cannot be negative, there will eventually be a remainder r_N which is equal to zero, at which point the algorithm stops. The remainder r_{N-1} is the GCD of a and b. If $(a < b)$ swap a and b before beginning the algorithm.

1.1.2 Euclid's Algorithm for finding modular inverses

Assume we have two integers a and b which are co-prime. We want to find the inverse of a $(mod\ b)$, denoted $\overline{a}$. We know from the definition of the modular inverse that $a\overline{a} \equiv 1\ (mod\ b)$. Hence our task is to solve the equation $ax + by = 1$ for x and y which will give us $x = \overline{a}$.

We do this by using Euclid's Algorithm and stopping when the remainder is equal to 1:

$$
\begin{aligned}
&a \ = \ q_0 b \ + \ r_0 \\
&b \ = \ q_1 r_0 \ + \ r_1 \\
&r_0 \ = \ q_2 r_1 \ + \ r_2 \\
&r_1 \ = \ q_3 r_2 \ + \ r_3 \\
&. \\
&. \\
&. \\
&r_{N-3} \ = \ q_{N-1} r_{N-2} \ + \ r_{N-1}
\end{aligned}
$$

We know that $r_{N-1} = 1$ because a and b are co-prime and hence their GCD is 1. We now re-write the equations and subtitute back until we end with an equation of the form $1 \ = \ ax \ + by$ and we will have $\overline{a} \ \equiv \ x \ (mod \ b)$.

1.2 Chinese Remainder Theorem

1.2.1 Statement

The Chinese Remainder Theorem states that the system of congruences,

$$
\begin{aligned}
&x \ \equiv \ a_1 \ (mod \ m_1) \\
&x \ \equiv \ a_2 \ (mod \ m_2) \\
&. \\
&. \\
&. \\
&x \ \equiv \ a_r \ (mod \ m_r)
\end{aligned}
$$

where the modulo $m_1, m_2, ..., m_r$ are all pairwise coprime has a unique solution modulo M given by

$$x \ \equiv \ a_1(M_1\overline{M_1}) + a_2(M_2\overline{M_2}) + ... + a_r(M_r\overline{M_r}) \ (mod \ M)$$

where

- $M = m_1 m_2 ... m_r$
- $M_i = \frac{M}{m_i}$
- $M_i\overline{M_i} \equiv 1 \ (mod \ m_i)$

1.2.2 Example 1

Let

$$
\begin{aligned}
&x \ \equiv \ 0 \ (mod \ 3) \\
&x \ \equiv \ 3 \ (mod \ 4) \\
&x \ \equiv \ 4 \ (mod \ 5)
\end{aligned}
$$

Find $x \ (modM)$

- $M \ = \ m_1 m_2 m_3 \ = \ (3)(4)(5) \ = \ 60$

- $M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$
  $M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$
  $M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$

- $$M_1\overline{M_1} \equiv 1\ (mod\ m_i)$$
  $$\Rightarrow 20\overline{M_1} \equiv 1\ (mod\ 3)$$
  $Using\ Euclid's\ Algorithm:$
  $Solving\ 1 = 20\overline{M_1} - 3y$
  $20 = 3(6) + 2$
  $3 = 2(1) + 1$
  $Substituting\ back:$
  $3 = (20 - 3(6))(1) + 1$
  $3 = 20(1) - 3(6) + 1$
  $1 = 3(7) + 20(-1)$
  Hence $\overline{M_1} \equiv -1\ (mod\ 3)$
  $\Rightarrow \overline{M_1} \equiv 2\ (mod\ 3)$

1.3 Modular Exponentiation Algorithm

1.3.1 Statement

To find the least postive residue of $a^n\ (modm)$ where n is a large number do the following:

- Express n in binary to get $n = (b_0)2^0 + (b_1)2^1 + (b_2)2^2 + ... + (b_k)2^k\ (b_i \in [0, 1])$
- Calculate the least positive residues modulo n for $a^{2^0},\ a^{2^1}, ...,\ a^{2^k}$
- Multiply the least positive residues whose corresponding bit is 1 in the first step.
- Find the least positive residue of the result above.

1.3.2 Example

What is the least positive residue of $3^231\ modulo\ 49$?

- 231 in binary:
  $231 = (1)2^7 + (1)2^6 + (1)2^5 + (0)2^4 + (0)2^3 + (1)2^2 + (1)2^1 + (1)2^0$
  Hence $231 = (11100111)_2$

- Least positive residues modulo 49 for $3^{2^0},\ 3^{2^1}, ...,\ 3^{2^7}$:
  $b_0 = 1$ $3^{2^0} \equiv 3^1 \equiv 3\ (mod\ 49)$
  $b_1 = 1$ $3^{2^1} \equiv 3^2 \equiv 9\ (mod\ 49)$
  $b_2 = 1$ $3^{2^2} \equiv 3^4 \equiv 9^2 \equiv 32\ (mod\ 49)$

$$\begin{array}{lllllll} b_3 = 0 & 3^{2^3} & \equiv & 3^8 & \equiv & 32^2 & \equiv \; 44 \; (mod\; 49) \\ b_4 = 0 & 3^{2^4} & \equiv & 3^{16} & \equiv & 44^2 & \equiv \; 25 \; (mod\; 49) \\ b_5 = 1 & 3^{2^5} & \equiv & 3^{32} & \equiv & 25^2 & \equiv \; 37 \; (mod\; 49) \\ b_6 = 1 & 3^{2^6} & \equiv & 3^{64} & \equiv & 37^2 & \equiv \; 46 \; (mod\; 49) \\ b_7 = 1 & 3^{2^7} & \equiv & 3^{128} & \equiv & 46^2 & \equiv \; 9 \; (mod\; 49) \end{array}$$

- Multiply results where $b_i = 1$:
  $(3)(9)(32)(37)(46)(9) = 13234752$
- Find least positive residue of above result:
  $3^{231} \equiv (3^{2^7})(3^{2^6})(3^{2^5})(3^{2^2})(3^{2^1})(3^{2^0}) \equiv 13234752 \equiv 48 \; (mod\; 49)$

1.3.3 Explanation of Algorithm

We know from the definition of the mod function that:

$$a \equiv r_1 \; (mod\; m)$$
$$b \equiv r_2 \; (mod\; m)$$
$$\Rightarrow ab \equiv r_1 r_2 \; (mod\; m)$$

This is what allows us to complete step 2 in the algorithm.

Furthermore, we know that $a^x a^y = a^{x+y}$ which is what allows us to split up the work in the algorithm and then recombine the results.

1.3.4 Fast-tracking the algorithm

Before applying the Modular Exponentiation Algorithm, we can eliminate a lot of the work by applying Euler's Theorem:
For any modulus n and integer a which are co-prime (ie GCD(a,n)=1) we have that:

$$a^{\varphi(m)} \equiv 1 \; (mod\; m)$$

Hence, to aid in computing the least positive residue we can express the exponent in the original problem as $n = q\varphi(m) + r$. This helps us in that we can now write $a^{q\varphi(m)+r}$ and since we know that $a^{\varphi} \equiv 1 \; (mod\; m)$ the problem is reduced to finding the least positive residue of $a^r \; (mod\; m)$. This is because $a^n \equiv a^{q\varphi(m)+r} \equiv a^{q\varphi(m)} a^r \equiv a^r \; (mod\; m)$.

2 Fermat's Factorization

2.0.1 Statement

Fermat's Factorization allows us to factorize an *odd* integer using the difference of two squares. Given an odd integer n, and two factors c and d s.t. $n = cd$ we know that:

$$n = (\frac{c+d}{2})^2 - (\frac{c-d}{2})^2$$

The method is as follows:

- We start by choosing $a = \lceil \sqrt{n} \rceil$
- We then calculate $n - a^2 = z$
- If z is a perfect square, we have found $b = \sqrt{z}$
- If z is not a perfect square, we increment a, and try again until we get a z which is a perfect square or we ascertain that n is a prime.
- Once we have a and b, the factors of n are calculated as:
  $c = a + b$
  $d = a - b$