CS 346 Class Notes

Mark Lindberg

Apr 4, 2016

This Time:

Corollary 8.21 to Theorem 8.14. For any $N > 1$, and $a \in \mathbb{Z}_N^*$, $a^{\phi(N)} = 1 \pmod N$.

Corollary 8.22 (to corollary 8.17): Fix $N > 1$. For any integer i, define $f_i : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ as $f_i(x) = x^i$. Let e be such that $\gcd(e, \phi(N)) = 1$, and let $d = e^{-1} \pmod{\phi(N)}$. Then f_d and f_e are permutations and f_d is the inverse of f_e.

The elements of $\mathbb{Z}_p^*$ are $1, 2, \ldots, p-1$ for p prime. If $N = p \cdot q$ for distinct primes p, q, then $|Z_N^*| = (p-1)(q-1)$.

Define: $\phi(N) = |\mathbb{Z}_N^*|$ for $N > 1$.

Modular exponentiation: $x^{1001101_2} = x^{10000000_2} \cdot x^{1000_2} \cdot x^{100_2} \cdot x^{1_2}$.

$x^{1_2} = x$.

$x^{10_2} = (x^{1_2})^2$.

$x^{100_2} = (x^{10_2})^2$.

And so on.

Chinese Remainder Theorem!

Group Isomorphism:

Let G and H be groups such that $|G| = |H|$.

Let the function $f : G \to H$ be a bijection, such that $\forall g_1, g_2 \in G$, $f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$.

It is an easy exercise to show that f^{-1} is a bijection from H to G.

We say that if such an f exists, G and H are isomorphic, $G \simeq H$.

CHINESE REMAINDER THEOREM:

Let p, q be distinct primes, $N = p \cdot q$. Then $\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q$, and $\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

The direct product $G \times H$ of two groups G, H.

The elements of $G \times H$ are (elements of G) $\times$ (elements of H).

The operation in $G \times H$: $(g_1, h_1) \circ (g_2, h_2) := (g_1 \circ_G g_2, h_1 \circ_H h_2)$.

In the CRT, the isomorphism f from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ is $f(x) := (x \pmod p, x \pmod q)$. The restriction of f to $\mathbb{Z}_n^*$ is an isomorphism from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$.

Applications of the CRT:

$14 \times 13 \pmod{15}$. Note that $N = 15$, and $14, 13 \in \mathbb{Z}_{15}^*$. Let $p = 5$, $q = 3$.

$14 \to (14 \pmod 5, 14 \pmod 3) = (4, 2)$.

$13 \to (13 \pmod 5, 14 \pmod 3) = (3, 1)$.

$(4, 2) \times (3, 1) = (4 \times 3 \pmod 5, 1 \times 2 \pmod 3) = (2, 2)$.

Now, find a $y \in \mathbb{Z}_1 5^*$ such that $y \pmod 5 = 2$, and $y \pmod 3 = 2$. Obviously, $y = 2$. (CRT guarantees exactly 1 element that satisfies this condition.)

For a fast way to do the other direction, when it's not so obvious, we can use the Extended Euclidean Algorithm to map (x_p, x_q) back to $x \in \mathbb{Z}_N^*$.

1. Solve the problem for $x_p = 1$, $x_q = 0$ to get $1_p \in \mathbb{Z}_N$.

   Solve the problem for $x_p = 0$, $x_q = 1$ to get $1_q \in \mathbb{Z}_N$.

   Find the X, Y such that $pX + qY = 1$. Then $1_p = X$, and $1_q = Y$.

2. $(x_p, x_q) \rightarrow x_p \cdot 1_p + x_q \cdot 1_q \pmod N$.

Can we factor in polynomial time?

The naive algorithm (testing up to the square root) is exponential in size of the number.

There is no known polynomial time algorithm.

For primality *testing*, however, we can work in polynomial time. Some of these algorithms have been known since the 1970s.

Prime number theorem: The number of primes in $\{1, \ldots, n\} \approx \frac{n}{\log(n)}$.

To gen an n-bit prime, pick a random n-bit value and check if prime. If not, repeat. We have the ability to efficiently generate large primes, and calculate N.