Lecture 14: Cryptography

Date: October 2, 2019.

Extended GCD Algorithm

Theorem 1 (Bézout). *For any integers a, b, $\gcd(a,b)$ is a linear combination of a and b, i.e., there are integers s, t such that $\gcd(a,b) = sa + tb$.*

To compute $\gcd(a,b)$, we can assume WLOG a, b are positive, and $a \geq b$.

```
gcd(a,b)
    x = a; y = b;
    s=1; t=0
    u=0; v=1
    while (y > 0)
        q = qcnt(x,y)
        r = rem(x,y)
        x = y
        y = r
        c=s; d=t
        s=u; t=v
        u=c-q.u; v=d-q.v
    return x (x,s,t,)
```

$a = x = 252$, $y = 198 = b$

$x = 1a + 0b$ $\quad y = 0a + 1b$

$x = 198 \quad y = 54$

$x = 0a + 1b \quad y = 252 - 1 \cdot 198 = 1a + (-1)b$

$x = 54 \quad y = 36$

$x = 1a + (-1)b \quad y = 198 - 3 \cdot 54 = (-3)a + 4 \cdot b$

$x = 36 \quad y = 18$

$x = 18 \quad y = 0$

Question 1. Is it the case that if $ab \equiv ac \pmod{n}$ then $b \equiv c \pmod{n}$?

$a = 2, b = 1, c = 3, n = 4.$

$2 \equiv 6 \pmod{4} \quad 1 \not\equiv 3 \pmod{4}$

Proposition 2. *For any integers a, b, c, n, if $\gcd(a,n) = 1$ and $ab \equiv ac \pmod{n}$ then $b \equiv c \pmod{n}$.*

Assume $\gcd(a,n) = 1$

$\exists s,t.\quad sa + tn = 1 \qquad tn \equiv 0 \pmod{n}$

$sa + tn \equiv 1 \pmod{n} \equiv sa \pmod{n}$

$ab \equiv ac \pmod{n}$

$sab \equiv sac \pmod{n}$

$b \equiv c \pmod{n}$

Multiplicative inverse of a modulo n is s if $sa \equiv 1 \pmod{n}$

3 has no multiplicative inverse mod 15.

Suppose s s.t. $3s \equiv 1 \pmod{15}$

$0 \equiv 15s \equiv 5 \pmod{15}$

Euler's Theorem

$\exists\ a \equiv b \pmod{n}$ but $c^a \not\equiv c^b \pmod{n}$

Relatively Prime: a is relatively prime to n if $\gcd(a,n) = 1$. $\mathbb{Z}_n^* = \{a \mid 0 \leq a < n \text{ AND } \gcd(a,n) = 1\}$.

Euler's Function: $\phi(n) = |\mathbb{Z}_n^*|$

Proposition 3. *1. For a prime p, $\phi(p) = p - 1$.*

2. For primes p, q, $\phi(pq) = (p-1)(q-1)$.

$\phi(p) = |\{a \mid 0 \leq a < p \text{ and } \gcd(a,p) = 1\}| = |\{1, 2, 3 \ldots p-1\}| = p - 1$

$\phi(pq) \qquad \{0, 1, 2, 3 \ldots\ldots pq-1\}^{pq}$

multiples of p: $0, p, 2p, \ldots (q-1)p$ — q

multiples of q: $0, q, 2q, \ldots (p-1)q$ — p

$\phi(pq) = pq - (p + q - 1) = (p-1)(q-1)$

Theorem 4 (Euler). *If* $\gcd(k,n) = 1$ *then*

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Fermat's Little Theorem : $0 \le a < p$ where p is prime, $a^{p-1} \equiv 1 \pmod{p}$

Non Theorem : If $a \equiv b \pmod{n}$ then $c^a \equiv c^b \pmod{n}$

Proposition 5. *For any (positive) integers* a, b, c, n *such that* $\gcd(c,n) = 1$ *and* $a \equiv b \pmod{\phi(n)}$ *then* $c^a \equiv c^b \pmod{n}$.

Assume, WLOG $b \geq a$. $a \equiv b \pmod{\phi(n)} \Rightarrow \phi(n) \mid b - a \Rightarrow b - a = k\phi(n)$

$$c^b = c^{a+(b-a)} = c^{a+k\phi(n)} = (c^a)(c^{k\phi(n)}) = (c^a)(c^{\phi(n)})^k$$
$$\equiv c^a \pmod{n}$$

Public Key Encryption (RSA) [Rivest-Shamir-Adelman 76/Cocks 73]

Messages: Each letter corresponds to a number, and message is the number obtained by concatenating all these digits. hello world

0805 - - - -

Receiver: Picks (large) primes p, q and $e \in \mathbb{Z}^*_{\phi(n)}$, where $n = pq$. Also computes d (secret key) such that $de \equiv 1 \pmod{\phi(n)}$. "Publishes" (n, e).

Sender: To send a message $M \in \mathbb{Z}^*_n$, compute $C = \text{rem}(M^e, n)$ and send C.

Receiver: To decrypt message C, compute $\text{rem}(C^d, n)$. Now,

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed \pmod{\phi(n)}} \pmod{n} \equiv M \pmod{n}$$