CS 13

Mathematical Foundations of Computing

RSA

Last Time

Another Theorem

Cancellation Property $\equiv_n$

If $\gcd(c, n) = 1$, then

$$ca \equiv_n cb \implies a \equiv_n b$$

.

Proof.

Since $\gcd(c, n) = 1$, it follows that there exists a c^{-1} such that $cc^{-1} + kn = 1$ for some $k \in \mathbb{Z}$.

Another Theorem

Cancellation Property $\equiv_n$

If $\gcd(c,n) = 1$, then

$$ca \equiv_n cb \implies a \equiv_n b$$

.

Proof.

Since $\gcd(c,n) = 1$, it follows that there exists a c^{-1} such that $cc^{-1} + kn = 1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned}
ca &\equiv_n cb \\
c^{-1}ca &\equiv_n c^{-1}cb && \text{[Multiplying both sides by } c^{-1}\text{]} \\
(1-kn)a &\equiv_n (1-kn)b && \text{[Definition of } c^{-1}\text{]} \\
a + kna &\equiv_n b + knb \\
a &\equiv_n b && [knX \equiv_n 0]
\end{aligned}$$

Define $Z_n^* = \{x \in \{1, \ldots, n-1\} \mid \gcd(x, n) = 1\}$.

Define
$\phi(n) = |Z_n^*|$ = "number of moduli of n that are relatively prime to n".

For $n = p$ where p is prime?

For $n = pq$ where $p \neq q$ and p, q are prime?

Permutation Property

Let $a \in Z_n^*$. Consider $Z_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$. Let $aZ_n^* = \{(ar_1) \text{ mod } n, (ar_2) \text{ mod } n, \ldots, (ar_{\phi(n)}) \text{ mod } n\}$.

We want to show that $Z_n^* = aZ_n^*$.

Proof ar_i mod $n \in Z_n^*$

It follows from the EEA that these integers exist and the corresponding equations are true: (1) $aa^{-1} + k_a n = 1$ (2) $r_i r_i^{-1} + k_{r_i} n = 1$

We would like to find integers ℓ and m such that:

$$ar_i \ell + mn = 1$$

Permutation Property

Let $a \in Z_n^*$. Consider $Z_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$. Let $aZ_n^* = \{(ar_1) \bmod n, (ar_2) \bmod n, \ldots, (ar_{\phi(n)}) \bmod n\}$.

We want to show that $Z_n^* = aZ_n^*$.

Proof $ar_i \bmod n \in Z_n^*$

It follows from the EEA that these integers exist and the corresponding equations are true: (1) $aa^{-1} + k_a n = 1$ (2) $r_i r_i^{-1} + k_{r_i} n = 1$

We would like to find integers ℓ and m such that:

$$ar_i \ell + mn = 1$$

Solving for aa^{-1} and $r_i r_i^{-1}$ and multiplying the results together:

$$aa^{-1} r_i r_i^{-1} = (1 - k_a n)(1 - k_{r_i} n)$$
$$aa^{-1} r_i r_i^{-1} = 1 - k_a n - k_{r_i} n + k_a k_{r_i} n^2$$
$$aa^{-1} r_i r_i^{-1} = (1 - n(k_a + k_{r_i} - k_a k_{r_i} n))$$

$$ar_i(a^{-1} r_i^{-1}) + n(k_a + k_{r_i} - k_a k_{r_i} n) = 1$$

Permutation Property

Let $a \in Z_n^*$. Consider $Z_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$. Let $aZ_n^* = \{(ar_1) \bmod n, (ar_2) \bmod n, \ldots, (ar_{\phi(n)}) \bmod n\}$.

We want to show that $Z_n^* = aZ_n^*$.

Proof of Uniqueness

Now, we prove $(ar_i \bmod n) \neq (ar_j \bmod n)$ for $i \neq j$. To do this, we show that when the moduli equal, $r_i = r_j$.

Permutation Property

Let $a \in Z_n^*$. Consider $Z_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$. Let $aZ_n^* = \{(ar_1) \text{ mod } n, (ar_2) \text{ mod } n, \ldots, (ar_{\phi(n)}) \text{ mod } n\}$.

We want to show that $Z_n^* = aZ_n^*$.

Proof of Uniqueness

Now, we prove $(ar_i \text{ mod } n) \neq (ar_j \text{ mod } n)$ for $i \neq j$. To do this, we show that when the moduli equal, $r_i = r_j$.

Suppose $ar_i \text{ mod } n = ar_j \text{ mod } n$. Then, $ar_i \equiv_n ar_j$. By the cancellation property from earlier this lecture, since $\gcd(a, n) = 1$, we have $r_i \equiv_n r_j$ as required.

We've already shown that

$$Z_n^* = aZ_n^*$$

We've already shown that

$$Z_n^* = aZ_n^*$$

Take the products of the elements of both sides:

$$\prod_{x \in Z_n^*} x \equiv_n \prod_{x \in aZ_n^*} x$$

We've already shown that

$$Z_n^* = aZ_n^*$$

Take the products of the elements of both sides:

$$\prod_{x \in Z_n^*} x \equiv_n \prod_{x \in aZ_n^*} x$$

Re-label terms:

$$\prod_{x \in Z_n^*} x \equiv_n a^{\phi(n)} \prod_{x \in Z_n^*} x$$

We've already shown that

$$Z_n^* = aZ_n^*$$

Take the products of the elements of both sides:

$$\prod_{x \in Z_n^*} x \equiv_n \prod_{x \in aZ_n^*} x$$

Re-label terms:

$$\prod_{x \in Z_n^*} x \equiv_n a^{\phi(n)} \prod_{x \in Z_n^*} x$$

Cancellation Theorem:

$$1 \equiv_n a^{\phi(n)}$$

$$1 \equiv_n a^{\phi(n)}$$