Number Theory & RSA

HW4 due
HW5 will be released tonight

Notation:

$\mathbb{Z}_n = \{0, \dots, n-1\}$ "integers mod n"

$x \% n$ = remainder when dividing x by n $[x \% n \in \mathbb{Z}_n]$

$x \mid n$: x divides n
n is a multiple of x
$n = k \cdot x$ for some integer k

$x \equiv_n y$: x & y are congruent mod n
$n \mid (x-y)$ alternative: $x \equiv y \pmod{n}$

$\gcd(x,y)$: greatest common divisor of x & y

Pari/GP: (installed on ENGR servers)

> gp

Mod(x,n)

"Division" mod n

Bezout theorem: let $d = \gcd(x,y)$, then you can write $d = ax + by$ where a & b are integers

Pari: bezout()

Suppose $\gcd(x,n)=1$

then $1 = ax + bn$ for integers a, b

$\downarrow$ reduce mod n

$1 \equiv_n ax + 0$

So x has a multiplicative inverse mod n which is "a" (can write $a \equiv_n x^{-1}$)

Def: $\mathbb{Z}_n^* \stackrel{def}{=} \{x \in \mathbb{Z}_n \mid \gcd(x,n) = 1\}$

then every element in $\mathbb{Z}_n^*$ has multiplicative inverse mod n

actually $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ has mult inverse}\}$

so multiplication & division make sense in $\mathbb{Z}_n^*$

Euler totient function

greek letter phi

$\varphi(n) \stackrel{def}{=} |\mathbb{Z}_n^*|$ = # of $x \in \mathbb{Z}_n$ relatively prime to n

Ex: $\varphi(11) = 10$

$\mathbb{Z}_{11} = \{0, \ldots, 10\}$

$\mathbb{Z}_{11}^* = \{\cancel{0}, 1, \ldots 10\}$

$\varphi(p) = p-1$ if p prime $\Rightarrow \mathbb{Z}_p^* = \{1, \ldots, p-1\}$

Ex: $\varphi(15) = 8$

$\mathbb{Z}_{15}$: $\cancel{0}$ 1 2 $\cancel{3}$ 4 $\cancel{5}$ $\cancel{6}$ 7 8 $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 14

mults of 3

mults of 5

If p, q primes $(p \neq q)$ then

$$\varphi(pq) = pq - (\#\text{ multiples of } p) - (\#\text{ multiples of } q) + 1$$

(because 0 is double counted)

$$= pq - q - p + 1$$

$$\varphi(pq) = (p-1)(q-1)$$

LaGrange Theorem:

for all $x \in \mathbb{Z}_n^*$, $x^{\varphi(n)} \equiv_n 1$

RSA:

$p \neq q$, primes

$N = p \cdot q$: "RSA modulus"

e, d where $e \cdot d \equiv_{\varphi(N)} 1$

(e, d multiplicative inverses mod $\varphi(N)$)

$\Rightarrow$ (N, e) is public key

(N, d) is private key

RSA function : $m \in \mathbb{Z}_N \longmapsto m^e \in \mathbb{Z}_N$

RSA inverse : $c \in \mathbb{Z}_N \longmapsto c^d \in \mathbb{Z}_N$

Claim: raise to the e power, then d power gets you back to where you started

Proof: $ed \equiv_{\varphi(N)} 1 \iff ed = k \cdot \varphi(N) + 1$ for some int k

$$(m^e)^d = m^{ed} = m^{k\varphi(N)+1}$$

$$= (m^{\varphi(N)})^k \cdot m$$

$$\equiv_N 1^k \cdot m = m$$