RSA

Don't forget Proj topics due WED 28th
(sorry for typo)

TODAY

- multiplicative inverses, Bezout
- totient, exponentiation
- RSA

} pari examples

$\mathbb{Z}_n$ vs $\mathbb{Z}_n^*$

$\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$

$\downarrow$ throw away mults of 3 & 5

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Claim: 7 has mult inverse mod 15

Bezout's theorem gives

(integers) $(-2)\cdot 7 + 1\cdot 15 = 1$

$\downarrow$ mod 15

$\underbrace{-2}_{\text{mult inverse of } 7} \cdot 7 \equiv_{15} 1$

$(-2 \equiv_{15} 13)$

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

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

Does 9 have inverse mod 15?

(shouldn't since $9 \notin \mathbb{Z}_{15}^*$)

$2\cdot 9 + (-1)\cdot 15 = 3 = \gcd(9, 15)$

$\downarrow$ mod 15

$2 \cdot 9 \equiv_{15} 3$

all true, but doesn't give you inverses

totient

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

$$\varphi(15) = \text{\# elements in } \{1, 2, 4, 7, 8, 11, 13, 14\}$$
$$= 8$$

$$\varphi(p) = p - 1 \quad \text{when } p \text{ is prime}$$

Euler's theorem:

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

(if $x^t \equiv_n 1$ then x^{t-1} is an inverse of x)

try: $n = 15$, $\varphi(n) = 8$

$$1^8 \longrightarrow 1$$
$$2^8 \longrightarrow 256 \bmod 15 = 1$$

Note: if operations are mod n, then all exponents can be reduced mod $\varphi(n)$

$$3^{141592} \bmod 11 \ ?$$

$$3^{141592} \equiv 3^{141592 \bmod 10} = 3^2 \equiv 9$$

Exponentiation with big numbers:

$x^{p-1} \mod p$?

too big!!!

- bad way: first compute $\underbrace{x^{p-1} \text{ OVER } \mathbb{Z}}$ then reduce mod p

Ex:

$$\boxed{\begin{array}{ll} \text{Computing } 13^{1024} & \\ \text{Bad way:} & \text{for } i=1 \text{ to } 1024 \\ & \quad x = 13 \cdot x \\ \text{good way:} & \text{for } i=1 \text{ to } 10 \\ & \quad x = x^2 \end{array}}$$

computing x^{37} $\quad (\overbrace{\underbrace{10010}_{18}}^{9}1)$

$$\begin{aligned} x^{37} &= x \cdot x^{36} \\ &= x \cdot (x^{18})^2 \\ &= x \cdot ((x^9)^2)^2 \\ &= x \cdot ((x \cdot x^8)^2)^2 \\ &= x \cdot ((x((x^2)^2)^2)^2)^2 \end{aligned}$$

- good way:

$$X^{37} \bmod n$$

$$X^{37} = x \cdot ((x((x^2)^2)^2)^2)^2 \bmod n$$

$$\ldots ((x \cdot (((x^2 \bmod n)^2 \bmod n)^2 \bmod n) \bmod n \ldots$$

Idea: If final result is needed mod n then can reduce intermediate values mod n

---

RSA:

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

$$ed \equiv_{\varphi(N)} 1$$

$$\underbrace{m \longrightarrow m^e \longrightarrow (m^e)^d = m}_{\text{all operations mod } N}$$