

Chinese Remainder Theorem

Start HW5 early!

RSA recap:

p, q distinct primes
 $N = pq$: RSA modulus
 e, d inverses mod $\phi(N)$

$$\left. \begin{array}{l} m \mapsto m^e \pmod{N} \\ c \mapsto c^d \pmod{N} \end{array} \right\} \text{inverses!}$$

Chinese Remainder Theorem:

let p, q be relatively prime $\left(\gcd(p, q) = 1 \right)$
then for all u, v , there
is a solution for x in

system
of eq'n's $\begin{cases} x \equiv_p u \\ x \equiv_q v \end{cases}$

Ex: $\begin{array}{l} x \equiv_5 2 \\ x \equiv_7 3 \end{array}$

Also, solution is unique mod pq

Alternatively:

$$x \in \mathbb{Z}_{pq} \xrightarrow{\text{crt}} (x \% p, x \% q) \in \mathbb{Z}_p \times \mathbb{Z}_q$$

this function is a bijection! (1-to-1 correspondence)

$$|\mathbb{Z}_{pq}| = p \cdot q = |\mathbb{Z}_p \times \mathbb{Z}_q|$$

Examples: $p=3, q=5$
(pari examples)

Ex: $p=3, q=5$

\mathbb{Z}_{15} world

$$\begin{array}{r} 7 \\ + 11 \\ \hline 3 \end{array}$$

$\text{mod } 15$

$$\xrightarrow{\text{crt}}$$

$$\xrightarrow{\text{crt}}$$

$$\xleftarrow{\text{crt}^{-1}}$$

$\mathbb{Z}_3 \times \mathbb{Z}_5$ world

$$(1, 2)$$

$$+ (2, 1)$$

$$\hline (0, 3)$$

$\text{mod } 3 \quad \text{mod } 5$

$$7$$

$$\begin{array}{r} + 13 \\ \hline 5 \end{array}$$

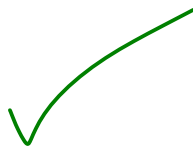
$$(1, 2)$$

$$(1, 3)$$

$$\hline (2, 0)$$

$$7$$

$$\begin{array}{r} * 11 \\ \hline 2 \end{array}$$



$$(1, 2)$$

$$* (2, 1)$$

$$\hline (2, 2)$$

Mathematically: \mathbb{Z}_{pq} and $\mathbb{Z}_p \times \mathbb{Z}_q$ are isomorphic
2 sets of "names" for same objects
(encodings)

Application to RSA:

RSA inverse $C \mapsto C^d \bmod N = p \cdot q$

p, q is $\approx 2k$ bits

\mathbb{Z}_{pq} world

C



p, q are $\approx k$ bits

$\mathbb{Z}_p \times \mathbb{Z}_q$ world

$(C \bmod p, C \bmod q)$

Cost:



$(2k)^3 = 8k^3$



$k^3 + k^3 = 2k^3$

C^d



$(C^d \bmod p, C^d \bmod q)$

Why?

Cost to compute $x \mapsto x^y \bmod n$
is roughly $(\# \text{ of bits in } n)^3$