Chinese Remainder Theorem

Start HW5 early!

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

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

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'ns $\begin{cases} x \equiv_p u \\ x \equiv_q v \end{cases}$

Ex: $x \equiv_5 2$
$x \equiv_7 3$

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: $p=3, \quad q=5$

$\mathbb{Z}_{15}$ world $\qquad\qquad$ $\mathbb{Z}_3 \times \mathbb{Z}_5$ world

$$\begin{array}{r} 7 \\ +\ 11 \\ \hline 3 \end{array} \qquad \begin{array}{c} \xrightarrow{crt} \\ \xrightarrow{crt} \\ \xleftarrow{crt^{-1}} \end{array} \qquad \begin{array}{r} (1,2) \\ +\ (2,1) \\ \hline (0,3) \end{array}$$

$$\underbrace{}_{\text{mod } 15} \qquad\qquad \underbrace{}_{\text{mod } 3}\ \underbrace{}_{\text{mod } 5}$$

1

$$\begin{array}{r} 7 \\ +\ 13 \\ \hline 5 \end{array} \qquad\qquad \begin{array}{r} (1,2) \\ (1,3) \\ \hline (2,0) \end{array}$$

$$\begin{array}{r} 7 \\ *\ 11 \\ \hline 2 \end{array} \qquad \checkmark \qquad \begin{array}{r} (1,2) \\ \times\ (2,1) \\ \hline (2,2) \end{array}$$

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 $\quad c \longmapsto c^d \mod N = p \cdot q$

pq is $\approx 2k$ bits — p, q are $\approx k$ bits

$\mathbb{Z}_{pq}$ world — $\mathbb{Z}_p \times \mathbb{Z}_q$ world

$$
\begin{tikzcd}
c \arrow[rr] \arrow[d, "(2k)^3 = 8k^3"] & & (c \,\%\, p,\ c \,\%\, q) \arrow[d, "k^3 + k^3 = 2k^3"] \\
c^d & & (c^d \,\%\, p,\ c^d \,\%\, q) \arrow[ll]
\end{tikzcd}
$$

Cost:

Why? Cost to compute $x \longrightarrow x^y \,\%\, n$ is roughly $(\#\text{ of bits in } n)^3$