Es 1

Let $p=11$, $q=19$, $n=pq=209$

How many solution does the equation $x^2 \equiv 171 \bmod 209$ have?

a) 1

b) 3

c) $\emptyset$ ✓

d) 4

e) 2

Solution: let p be a prime and r an integer not divisible by p. Then r is a quadratic residue mod p iff

$$r^{\frac{p-1}{2}} \equiv 1 \bmod p$$

The group of all quadratic residues is $1^2, 2^2, 3^2, \dots \left(\frac{p-1}{2}\right)^2$

Let $x^2 \equiv r \bmod n$

If $r=0$, then $\exists!\ x \equiv 0 \bmod n$

If $r>0$:

Use CRT to split the equation in other 2nd degree equations $x^2 \equiv a \bmod p^k$ with p odd and $\gcd(a,p)=1$

- NO SOLUTIONS if $\left(\frac{a}{p}\right)=-1$ (if a is not a quadratic residue mod$p$
- 2 SOLUTIONS x_1, x_2 if $\left(\frac{a}{p}\right)=1$ (if a is a quadratic residue mod$p$)
- $x^2 \equiv a \bmod 2^k$:
  - if $k=1 \Rightarrow$ UNIQUE solution $x \equiv 1 \bmod 2$
  - $k=2 \Rightarrow$ no solution if $a=3$ or there are 2 solutions $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv 3 \bmod 4$ if $a \equiv 1 \bmod 4$
  - $k=3 \Rightarrow$ no solution if $a \equiv 1 \bmod 2^k$ or there are 4 solutions $x_1, -x_1, x_1+2^{k-1}, -(x_1+2^{k-1})$ if $a \equiv 1 \bmod 2^3$

In this case we exploit $209 = 19 \times 11 \Rightarrow$ CRT

$$\begin{cases} x^2 = 171 \equiv 6 \bmod 11 \\ x^2 = 171 \equiv \emptyset \bmod 19 \end{cases} \Rightarrow \exists!\ x \equiv 0 \bmod 19$$

If we substitute $\Rightarrow 0 \not\equiv 6 \bmod 11$

$\Rightarrow$ NO SOLUTIONS!

Es 1 other version

$p=11,\ q=19,\ pq=209$

How many solutions does $x^2 \equiv 130 \mod 209$ have?

a) 1

b) 4 ✓

c) 2

d) 3

e) $\emptyset$

Solution: use CRT to split the equation

$$\begin{cases} x^2 \equiv 9 \mod 11 \\ x^2 \equiv 16 \mod 19 \end{cases}$$

$x \equiv \pm 3 \mod 11$
$x \equiv \pm 4 \mod 19$

Check if they are quadratic residues

$9^{\frac{11-1}{2}} \equiv 1 \mod 11 ? \Rightarrow 9^5 = 9^2 \cdot 9 \cdot 9^2 = 4 \cdot 4 \cdot 9 = 5 \cdot 9 \equiv 1 \mod 11$ OK

$16^{\frac{19-1}{2}} \equiv 1 \mod 19 ? \Rightarrow 16^9 = 16^2 \cdot 16^7 = 16^2 \cdot 16^2 \cdot 16^2 \cdot 16^2 \cdot 16 = 9 \cdot 9 \cdot 9 \cdot 9 \cdot 16$

$= 5 \cdot 5 \cdot 16 = 6 \cdot 16 = 6 \cdot 4 \cdot 4 \equiv 1 \mod 19$ OK

Es 2

Let $f: \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ be the isomorphism of CRT, then

a) $f(x,y) = 7x + 9y$

b) $f(x,y) = 6x + 10y$

c) $f(x,y) = 10x + 6y$ ✓

d) $f(x,y) = 12x + 4y$

Solution:

CRT: Assume n_1, n_2 coprime, i.e $\gcd(n_1, n_2) = 1$. Let x be the solution to the following systems of modulo identities

$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$

Then $x = (X_2 n_2 a_1 + X_1 n_1 a_2) \bmod N$, where $N = n_1 \times n_2$ and $X_1 n_1 + X_2 n_2 = 1$

$\Rightarrow$ bijection between $\mathbb{Z}_p \times \mathbb{Z}_q$

$\left.\begin{matrix} n_1 = 3 \\ n_2 = 5 \end{matrix}\right\} N = 15$

Example : $9 \bmod 15 \Rightarrow (0, 4)$

$\mathbb{Z}_{15} = \underset{x}{\mathbb{Z}_3} \times \underset{y}{\mathbb{Z}_5}$

$7 \times 0 + 9 \times 4 = 36 \equiv 6 \bmod 15$ NO
$6 \times 0 + 10 \times 4 = 40 \equiv 10 \bmod 15$ NO

$10x + 6y = 24 \equiv 9 \bmod 15$

Another method

$f(a,b) = a f(1,0) + b f(0,1)$ Linear Combination

$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 0 \bmod 5 \end{cases}$

If $x \equiv 0 \bmod 5$, then $x = 5y$

$5y \equiv 1 \bmod 3$

$\Rightarrow y = 5^{-1} \bmod 3 = 2$

$x = 5y = 10$

Es 2 other version

Let $f: \mathbb{Z}_5 \times \mathbb{Z}_7 \to \mathbb{Z}_{35}$ be the isomorphism of the CRT. Then

a) $f(x,y) = 20x + 16y$

b) $f(x,y) = 21x + 15y$ ✓

c) $f(x,y) = 15x + 21y$

d) $f(x,y) = 17x + 19y$

Solution: brute force approach

Example: $9 \bmod 35 \to \equiv 4 \bmod 5$, $\equiv 2 \bmod 7$

$$9 \longrightarrow (\overset{x}{4}, \overset{y}{2})$$

$20x + 16y = 10 + 32 = 7$ NO
$21x + 15y = 14 + 30 = 9$ ok

$$f(a,b) = af(1,0) + bf(0,1)$$

$$\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 0 \bmod 7 \end{cases} \Rightarrow x \equiv 7y$$

$7y \equiv 1 \bmod 5$

$y \equiv 7^{-1} \bmod 5 = 3$

$x = 21$

$f(x,y) = 21x + 15y$

Es 3

Alice generates a secret key $sk_A = 4$ and wants to generate a DS. Prime numbers $p = 11$, $q = 5$

What is the public key?

Solution: key generation for DSA

- generate a prime $p \Rightarrow p = 11$
- find a prime divisor q of $p-1$
  $p-1 = 10 \Rightarrow q = 5$
- find an element α with $ord(\alpha) = q$, i.e α generates the subgroup with q elements
  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \Rightarrow \alpha = 3$
  $\alpha^q \equiv 1 \bmod q \Rightarrow 3^5 = 3^2 \cdot 3^3 = 4 \cdot 4 \cdot 3 \equiv 1 \bmod 5$
- Choose a random integer d with $0 < d < q$
  $d = 4$
- compute $\beta = \alpha^d \bmod p = 3^4 \bmod 11 = 9 \cdot 3 \cdot 3 \equiv 4$

The public key is $K_{pub} = (p, q, \alpha, \beta) = (11, 5, 3, 4)$