Discrete Square Root

Discrete Square Root Problem

- The **discrete square root problem** is defined as the computation of $x \in \mathcal{Z}_n$ in
$$y = x^2 \pmod n$$
given n and y
- Depending on whether n is composite or prime, we have problems of different complexity
- First consider the case where the modulus is prime, for example, take $p = 11$, and square all group elements in $\mathcal{Z}_{11}^*$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

Discrete Square Root Mod p

- The square root of y modulo 11 may not exist for all y values, for example, $x^2 = y \pmod{11}$ for $y = 2, 6, 7, 8, 10$ does not have any solutions
- In general, the solution of $x^2 = y \pmod p$ does not exist for $(p-1)/2$ values of y which are called quadratic nonresidues (QNR)
- If there is a square root x of y modulo 11, then $-x \pmod{11}$ is also a square root since $x^2 = (-x)^2 = y \pmod p$, for example, $2^2 = (-2)^2 = 9^2 = 4 \pmod{11}$ or $3^2 = (-3)^2 = 8^2 = 9 \pmod{11}$
- Two solutions x and $-x$ of $x^2 = y \pmod p$ exist for the remaining $(p-1)/2$ values of y which are called quadratic residues (QR)

Discrete Square Root for $p = 3 \pmod 4$

- Solving for $x = \sqrt{y} \pmod p$ for a prime p
- First, determine if there is a solution, i.e., if y is QR mod p
- Euler's theorem provides a simple test:

$$u = y^{(p-1)/2} \pmod p \quad \rightarrow \quad \begin{cases} u = 1 & \text{if} \quad y \quad \text{is QR} \\ u = -1 & \text{if} \quad y \quad \text{is QNR} \end{cases}$$

- If there is a solution, it can be found very quickly for half of the primes, namely, for primes with property $p = 3 \pmod 4$, by computing

$$x = y^{(p+1)/4} \pmod p$$

Discrete Square Root Mod p Example

- Example: $x^2 = 5 \pmod{11}$
- Euler's Theorem: $y^{(p-1)/2} = 5^{(11-1)/2} = 5^5 = 1 \pmod{11}$
- Since $11 = 3 \pmod 4$, the solution is easily found as

$$x = y^{(p+1)/4} = 5^{(11+1)/4} = 5^3 = 125 = 4 \pmod{11}$$

  Therefore, $x = \{4, -4\} = \{4, 7\}$ are the solutions of $x^2 = 5 \pmod{11}$
- What about the solution of $x^2 = 2 \pmod{11}$
  Euler's Theorem: $y^{(p-1)/2} = 2^{(11-1)/2} = 2^5 = 32 = -1 \pmod{11}$
  There is no solution for x in $x^2 = 2 \pmod{11}$

Discrete Square Root for $p = 1 \pmod 4$

- To compute a square root mod p for primes $p = 1 \pmod 4$, we first factor $p - 1$ and find s and odd m such that $p - 1 = 2^s \cdot m$
- The algorithm starts with a random QNR, and finds $x = \sqrt{y} \bmod p$

  Take a random QNR z, i.e., $\{ z \mid z^{(p-1)/2} = -1 \pmod p \}$

```
a = y^m (mod p)
x = y^((m+1)/2) (mod p)
b = z^m (mod p)
for i = s-1, s-2, ..., 1
    if a^(2^(i-1)) = -1 (mod p)
        a = a · b^2
        x = x · b
    b = b^2
return x
```

Discrete Square Root Mod p Example

- Prime $p = 673$, with $673 = 1 \pmod 4$, and find $\sqrt{83} \pmod{673}$
  Take $z = 5$, a QNR since $5^{(673-1)/2} = 5^{336} = -1 \pmod{673}$
  $673 - 1 = 2^5 \cdot 21$, therefore, $s = 5$ and $m = 21$

i	$a^{2^{i-1}}$	a	x	b
		$83^{21} = 589$	$83^{(21+1)/2} = 190$	$5^{21} = 118$
4	$589^{2^3} = -1$	$589 \cdot 118^2 = 58$	$190 \cdot 118 = 211$	$118^2 = 464$
3	$58^{2^2} = 1$	58	211	$464^2 = 609$
2	$58^{2^1} = -1$	$58 \cdot 609^2 = 672$	$211 \cdot 629$	$609^2 = 58$
1	$672^{2^0} = -1$	$672 \cdot 58^2 = 1$	$629 \cdot 58 = 140$	$58^2 = -1$

- Thus, we find the square root of 83 as $x = 140$, which satisfies

$$140^2 = 83 \pmod{673}$$

Discrete Square Root Mod n

- If $n = pq$, and we know the prime factors p and q, then the square root problem mod n can be converted into two separate square root problems mod p and mod q using the Chinese Remainder Theorem:

$$x^2 = y \pmod{pq} \quad \text{implies} \quad \begin{cases} x^2 = y \pmod{p} \\ x^2 = y \pmod{q} \end{cases}$$

  We can then solve these two equations, and find two square roots from the first equation $\{x_p, -x_p\}$ and two square roots from the second equation $\{x_q, -x_q\}$, and combine them using the CRT

- There are 4 square roots of y modulo n for $n = pq$

$$\begin{array}{cc} \mathrm{CRT}(x_p, x_q; p, q) & \mathrm{CRT}(x_p, -x_q; p, q) \\ \mathrm{CRT}(-x_p, x_q; p, q) & \mathrm{CRT}(-x_p, -x_q; p, q) \end{array}$$

Discrete Square Root Mod n

- Consider solving for $x^2 = 177 \pmod{209}$ for $n = pq = 11 \cdot 19$
- Break them two separate square root problems with the help of the CRT:

$$x^2 = 177 \pmod{11 \cdot 19} \quad \text{implies} \quad \begin{cases} x^2 = 177 = 1 & \pmod{11} \\ x^2 = 177 = 6 & \pmod{19} \end{cases}$$

- The solution of $x^2 = 1 \pmod{11}$ is found easily as $\{1, -1\}$
  The solution of $x^2 = 6 \pmod{19}$ is found as $\{5, -5\}$:

$$x = y^{(p+1)/4} = 6^{(19+1)/4} = 6^5 = 5 \pmod{19}$$

- The CRT on 4 combinations: $(1, 5)$, $(1, -5)$, $(-1, 5)$, and $(-1, -5)$

Simplified CRT with Two Primes

- Given the residues (r_p, r_q) of an integer x with respect to the primes (p, q), the CRT gives us x as

$$x = r_p \cdot c_1 \cdot \frac{pq}{p} + r_q \cdot c_2 \cdot \frac{pq}{q} = r_p \cdot c_1 \cdot q + r_q \cdot c_2 \cdot p \pmod{pq}$$

  such that $c_1 = q^{-1} \pmod p$ and $c_2 = p^{-1} \pmod q$
- If we run the extended Euclidean algorithm with p and q as inputs, we will obtain the integers a and b such that $a \cdot p + b \cdot q = 1$, which implies that $a = p^{-1} = c_2 \pmod q$ and $b = q^{-1} = c_1 \pmod p$
- Therefore, the simplified CRT formula for two primes becomes

$$r_p \cdot b \cdot q + r_q \cdot a \cdot p \pmod{pq}$$

Discrete Square Root Mod n Example

- Applying the EEA for the primes $p = 11$ and $q = 19$, we find

$$7 \cdot 11 - 4 \cdot 19 = 1$$

we find $a = 7$ and $b = -4$, and thus, write the CRT sum as

$$r_p \cdot (-4) \cdot 19 + r_q \cdot 7 \cdot 11 = -76 \cdot r_p + 77 \cdot r_q \pmod{209}$$

- Using this formula on the 2 combinations of square roots, we find

$$\begin{aligned} \mathrm{CRT}(1,5) &= (-76) \cdot 1 + 77 \cdot 5 = 100 \pmod{209} \\ \mathrm{CRT}(-1,5) &= (-76) \cdot (-1) + 77 \cdot 5 = 43 \pmod{209} \end{aligned}$$

The other 2 solutions will be the negatives of these numbers mod 209, and thus, the square roots are $\{43, 100, -43, -100\}$