Information & System Security

Lecture 26

VIT-AP
UNIVERSITY

Mathematics Related to Public Key Cryptography

9-3 FACTORIZATION

- ***Factorization has been the subject of continuous research in the past; such research is likely to continue in the future.***
- ***Factorization plays a very important role in the security of several public-key cryptosystems (see Chapter 10).***

Topics discussed in this section:

9.3.1 Fundamental Theorem of Arithmetic
9.3.2 Factorization Methods
9.3.3 Fermat Method

9.3.1 Fundamental Theorem of Arithmetic

$$n = p_1^{e1} \times p_2^{e2} \times \cdots \times p_k^{ek}$$

Greatest Common Divisor

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} \qquad b = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{bk}$$

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \times p_2^{\min(a_2, b_2)} \times \cdots \times p_k^{\min(a_k, b_k)}$$

Least Common Multiplier

$$a = p_1^{a1} \times p_2^{a2} \times \cdots \times p_k^{ak} \qquad b = p_1^{b1} \times p_2^{b2} \times \cdots \times p_k^{bk}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \times p_2^{\max(a_2, b_2)} \times \cdots \times p_k^{\max(a_k, b_k)}$$

$$\operatorname{lcm}(a, b) \times \gcd(a, b) = a \times b$$

9.3.2 Factorization Methods

Trial Division Method

```
Trial_Division_Factorization (n)   // n is the number to be factored
{
    a ← 2
    while (a ≤ √n )
    {
        while (n mod a = 0)
        {
            output a                // Factors are output one by one
            n = n / a
        }
        a ← a + 1
    }
    if (n > 1) output n             // n has no more factors
}
```

Example

Use the trial division algorithm to find the factors of 1233.

Solution

We use the trial division algorithm and get the following result.

$$1233 = 3^2 \times 137$$

Example

Use the trial division algorithm to find the factors of 1523357784.

Solution

We use the trial division algorithm and get the following result.

$$1523357784 = 2^3 \times 3^2 \times 13 \times 37 \times 43987$$

9.3.3 Fermat's Method

$$n = x^2 - y^2 = a \times b \text{ with a} = (\text{x} + \text{y}) \text{ and b} = (\text{x} - \text{y})$$

```
Feramat_Factorization (n)    // n is the number to be factored
{
    x ← √n          // smallest integer greater than √n
    while (x < n)
    {
      w ← x² − n
      if (w is perfect square)
      {
        y ← √w;  a ← x + y;
        b ← x − y;   return a and b
      }
     x ← x + 1
    }
}
```

Example

Use the Fermat's method to find the factors of 33.

Solution

We use the Fermat's method and get the following result.

$n=33$, $x=\text{ceil}(\sqrt{n})=\text{ceil}(\sqrt{33})=6$.

Itr	x	$w=x^2-n$	is w perf sqr	$y=\sqrt{w}$	(x+y) a	(x-y) b
1	6	3	no	-	-	-
2	7	16	yes	4	11	3

Factors of 33 are 3 and 11.

Example

Use the Fermat's method to find the factors of 123.

Solution

We use the Fermat's method and get the following result.

$n = 123$, $x = \text{ceil}(\sqrt{n}) = \text{ceil}(\sqrt{123}) = 12$

Itr	x	$w=x^2-n$	w perf sq	$y=\sqrt{w}$	a=x+y	b=x-y
1	12	21	no	-	-	-
2	13	46	no	-	-	-
3	14	63	no	-	-	-
…	…	…	…	…	…	…
11	22	361	yes	19	41	3

9-4 CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.

2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.

3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.

4. The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

Example

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$
3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$
4. $X = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$
   $= 23 \bmod 105$

Example

Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

Solution

This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

If we follow the four steps, we find x = 276.
We can check that 276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is 0).

Example

Assume we need to calculate $z = x + y$ where $x = 123$ and $y = 334$, but our system accepts only numbers less than 100. These numbers can be represented as follows:

$$x \equiv 24 \pmod{99} \qquad y \equiv 37 \pmod{99}$$
$$x \equiv 25 \pmod{98} \qquad y \equiv 40 \pmod{98}$$
$$x \equiv 26 \pmod{97} \qquad y \equiv 43 \pmod{97}$$

Solution

Adding each congruence in x with the corresponding congruence in y gives

$$x + y \equiv 61 \pmod{99} \quad \rightarrow \quad z \equiv 61 \pmod{99}$$
$$x + y \equiv 65 \pmod{98} \quad \rightarrow \quad z \equiv 65 \pmod{98}$$
$$x + y \equiv 69 \pmod{97} \quad \rightarrow \quad z \equiv 69 \pmod{97}$$

Now three equations can be solved using the Chinese remainder theorem to find z. One of the acceptable answers is $z = 457$.

9-5 QUADRATIC CONGRUENCE

- ***In cryptography, we also need to discuss quadratic congruence—that is, equations of the form $a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}$.***
- ***We limit our discussion to quadratic equations in which $a_2 = 1$ and $a_1 = 0$, that is equations of the form***

$$\boxed{x^2 \equiv a \pmod{n}.}$$

Topics discussed in this section:

9.5.1 Quadratic Congruence Modulo a Prime
9.5.2 Quadratic Congruence Modulo a Composite

9.5.1 Quadratic Congruence Modulo a Prime

We first consider the case in which the modulus is a prime.

Example **The equation $x^2 \equiv 3 \pmod{11}$ has two solutions, $x \equiv 5 \pmod{11}$ and $x \equiv -5 \pmod{11}$. But note that $-5 \equiv 6 \pmod{11}$, so the solutions are actually 5 and 6. Also note that these two solutions are incongruent.**

Example **The equation $x^2 \equiv 2 \pmod{11}$ has no solution. No integer x can be found such that its square is 2 mod 11.**

9.5.1 Continued

Quadratic Residues and Nonresidue

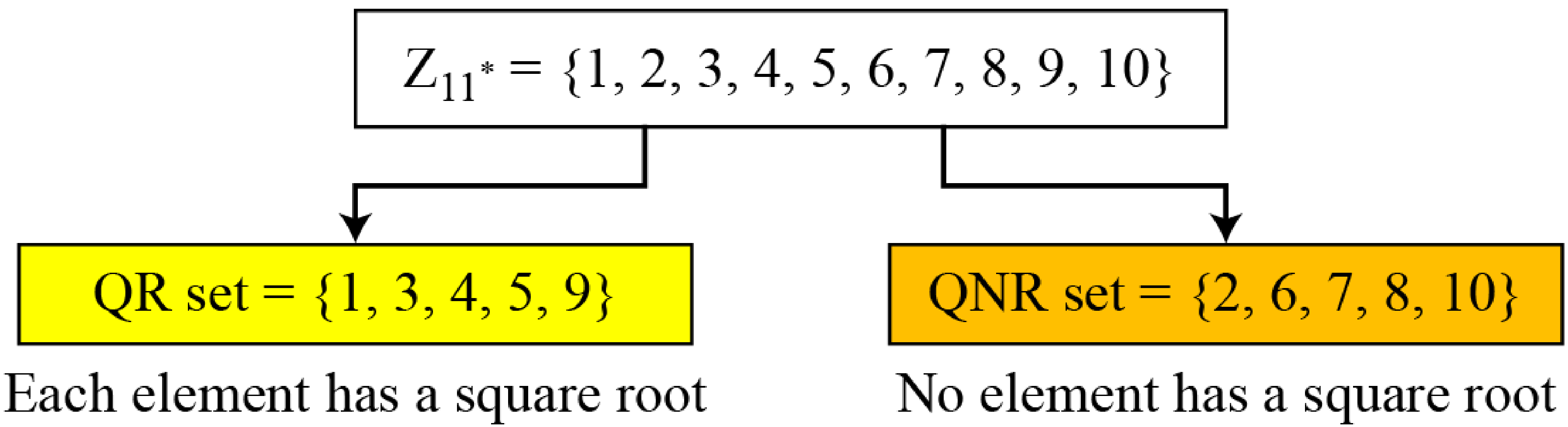
In the equation $x^2 \equiv a \pmod{p}$, a is called

- ***a quadratic residue (QR) if the equation has two solutions;***
- ***a quadratic nonresidue (QNR) if the equation has no solutions.***

9.5.1 Continued

Example

There are 10 elements in Z_{11}*. Exactly five of them are quadratic residues and five of them are nonresidues. In other words, Z_{11}* is divided into two separate sets, QR and QNR, as shown in Figure.



Division of Z_{11}* elements into QRs and QNRs

9.5.1 Continued

Euler's Criteria

a. ***If $a^{(p-1)/2} \equiv 1 \pmod p$, a is a quadratic residue modulo p.***

b. ***If $a^{(p-1)/2} \equiv -1 \pmod p$, a is a quadratic nonresidue modulo p.***

Example

To find out if 14 or 16 is a QR in Z_{23}*, we calculate:

$14^{(23-1)/2}$ mod 23 → 22 mod 23 → −1 mod 23 (nonresidue)

$16^{(23-1)/2}$ mod 23 → 16^{11} mod 23→ 1 mod 23 (residue)

Solving Quadratic Equation Modulo a Prime

Special Case: $p = 4k + 3$

Solutions:

$$\boxed{x \equiv a^{(p+1)/4} \pmod{p} \text{ and } x \equiv -a^{(p+1)/4} \pmod{p}}$$

9.5.1 Continued

Example

Solve the following quadratic equations:

a. $x^2 \equiv 3 \pmod{23}$
b. $x^2 \equiv 2 \pmod{11}$
c. $x^2 \equiv 7 \pmod{19}$

Solutions

a. $x \equiv \pm 16 \pmod{23}$ $\sqrt{3} \equiv \pm 16 \pmod{23}$.

b. There is no solution for $\sqrt{2}$ in Z_{11}.

c. $x \equiv \pm 11 \pmod{19}$. $\sqrt{7} \equiv \pm 11 \pmod{19}$.

9.5.2 Quadratic Congruence Modulo a Composite

$$x^2 \equiv a \bmod (n)$$
$$n = p_1 \times p_2 \times \ . \ . \ . \times p_k$$

$$x^2 \equiv a_1 \pmod{p_1}$$
$$x^2 \equiv a_2 \pmod{p_2}$$
$$\cdots$$
$$x^2 \equiv a_k \pmod{p_k}$$

$$x_1 \equiv \pm\, b_1 \pmod{p_1}$$
$$x_2 \equiv \pm\, b_2 \pmod{p_2}$$
$$\cdots$$
$$x_k \equiv \pm\, b_k \pmod{p_k}$$

Decomposition of congruence modulo a composite

9.5.2 *Continued*

Example

Assume that $x^2 \equiv 36 \pmod{77}$. We know that $77 = 7 \times 11$. We can write

$$x^2 \equiv 36 \pmod 7 \equiv 1 \pmod 7 \quad \text{and} \quad x^2 \equiv 36 \pmod{11} \equiv 3 \pmod{11}$$

The answers are $x \equiv +1 \pmod 7$, $x \equiv -1 \pmod 7$, $x \equiv +5 \pmod{11}$, and $x \equiv -5 \pmod{11}$. Now we can make four sets of equations out of these:

Set 1: $x \equiv +1 \pmod 7$ $\quad x \equiv +5 \pmod{11}$

Set 2: $x \equiv +1 \pmod 7$ $\quad x \equiv -5 \pmod{11}$

Set 3: $x \equiv -1 \pmod 7$ $\quad x \equiv +5 \pmod{11}$

Set 4: $x \equiv -1 \pmod 7$ $\quad x \equiv -5 \pmod{11}$

The answers are $x = \pm 6$ and ± 27.

Complexity

How hard is it to solve a quadratic congruence modulo a composite?

The main task is the factorization of the modulus. In other words, the complexity of solving a quadratic congruence modulo a composite is the same as factorizing a composite integer. As we have seen, if *n* is very large, factorization is infeasible.

Note

Solving a quadratic congruence modulo a composite is as hard as factorization of the modulus.

References

- **Chapter 9 -** Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.

- **Chapter 8 -** William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.