VE203
Discrete Math
RC5

Yucheng Huang

University of Michigan
Shanghai Jiao Tong University
Joint Institute

March 30, 2022

Ring

Definition

A ring $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied:

$\mathscr{R}_1$.$\langle R, + \rangle$ is an abelian group.

$\mathscr{R}_2$. Multiplication is associative.

$\mathscr{R}_3$. For all $a, b, c \in R$, the left distributive law, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the right distributive law $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Ring

We are well aware that axioms $\mathscr{R}_1, \mathscr{R}_2$, and $\mathscr{R}_3$ for a ring hold in any subset of the complex numbers that is a group under addition and that is closed under multiplication. For example, $\langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{Q}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$ are rings.

Ring

Consider the cyclic group $\langle \mathbb{Z}_n, + \rangle$. If we define for $a, b \in \mathbb{Z}_n$ the product ab as the remainder of the usual product of integers when divided by n, it can be shown that $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring. We shall feel free to use this fact. For example, in $\mathbb{Z}_{10}$ we have $(3)(7) = 1$. This operation on $\mathbb{Z}_n$ is multiplication modulo n. We do not check the ring axioms here. From now on, $\mathbb{Z}_n$ will always be the ring $\langle \mathbb{Z}_n, +, \cdot \rangle$.

Property

If R is a ring with additive identity 0 , then for any $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

Property

For Property 1 , note that by axioms $\mathscr{R}_1$ and $\mathscr{R}_2$,

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Then by the cancellation law for the additive group $\langle R, + \rangle$, we have $a0 = 0$. Likewise,

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a$$

implies that $0a = 0$. This proves Property 1 . In order to understand the proof of Property 2 , we must remember that, by definition, $-(ab)$ is the element that when added to ab gives 0 . Thus to show that $a(-b) = -(ab)$, we must show precisely that $a(-b) + ab = 0$. By the left distributive law,

$$a(-b) + ab = a(-b + b) = a0 = 0$$

since $a0 = 0$ by Property 1 . Likewise,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

Property

For Property 3, note that

$$(-a)(-b) = -(a(-b))$$

by Property 2 . Again by Property 2 ,

$$-(a(-b)) = -(-(ab)),$$

and $-(-(ab))$ is the element that when added to $-(ab)$ gives 0 . This is ab by definition of $-(ab)$ and by the uniqueness of an inverse in a group. Thus, $(-a)(-b) = ab$.

Homomorphism

For rings R and R', a map $\phi : R \to R'$ is a homomorphism if the following two conditions are satisfied for all $a, b \in R$:

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$.

Exercise 1

In Exercises 1 through 6, compute the product in the given ring.

1. $(12)(16)$ in $\mathbb{Z}_{24}$
2. $(16)(3)$ in $\mathbb{Z}_{32}$
3. $(11)(-4)$ in $\mathbb{Z}_{15}$
4. $(20)(-8)$ in $\mathbb{Z}_{26}$
5. $(2,3)(3,5)$ in $\mathbb{Z}_5 \times \mathbb{Z}_9$
6. $(-3,5)(2,-4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{11}$

Exercise 1 Solution

1. 0
2. 16
3. 1
4. 22
5. $(1, 6)$
6. $(2, 2)$

Exercise 2

Decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case.

1. $n\mathbb{Z}$ with the usual addition and multiplication
2. $\mathbb{Z}^+$with the usual addition and multiplication
3. $\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components
4. The set of all pure imaginary complex numbers ri for $r \in \mathbb{R}$ with the usual addition and multiplication

Exercise 2 Solution

1. Yes, $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$ is a commutative ring.
2. No, $\mathbb{Z}^+$ is not a ring; there is no identity for addition.
3. Yes, $\mathbb{Z} \times \mathbb{Z}$ is a commutative ring.
4. No, $\mathbb{R}i$ is not closed under multiplication.

Exercise 3

Show that $a^2 - b^2 = (a+b)(a-b)$ for all a and b in a ring R if and only if R is commutative.

Exercise 3 Solution

Now $(a+b)(a-b) = a^2 + ba - ab - b^2$ is equal to $a^2 - b^2$ if and only if $ba - ab = 0$, that is, if and only if $ba = ab$. But $ba = ab$ for all $a, b \in R$ if and only if R is commutative.

1. Ring (Optional)
2. Modular Arithmetic
   - Modulo
   - Fermat's (Little) Theorem
   - Congruences
   - Fast Modular Exponentiation
   - Chinese Remainder Theorem
   - RSA Cryptography
3. Q&A

1. Ring (Optional)
2. Modular Arithmetic
   - Modulo
   - Fermat's (Little) Theorem
   - Congruences
   - Fast Modular Exponentiation
   - Chinese Remainder Theorem
   - RSA Cryptography
3. Q&A

Modular Arithmetic

Definition

Given $a, b \in \mathbb{Z}$, a and b are said to be congruent modulo n, i.e.,

$$a \equiv b (\bmod n)$$

if $n \mid b - a$, i.e., $b = a + nk$ for some $k \in \mathbb{Z}$

Modular Arithmetic

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6 .

Solution: Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod 6$. However, because $24 - 14 = 10$ is not divisible by 6 , we see that $24 \not\equiv 14 (\mathrm{mod} 6)$.

Theorem 1

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

and

$$ac \equiv bd \pmod{m}$$

Proof: We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$$

Hence,

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}$$

Example

Because $7 \equiv 2 (\mathrm{mod} 5)$ and $11 \equiv 1 (\mathrm{mod} 5)$, it follows from Theorem 1 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 (\mathrm{mod} 5)$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 (\mathrm{mod} 5)$$

Exercise 4

Find each of these values.

a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

Exercise 4 Solution

a) Working modulo 23 , we have $-133 + 261 = 128 \equiv 13$, so the answer is 13 .

b) Working modulo 23 , we have $457 \cdot 182 \equiv 20 \cdot 21 = 420 \equiv 6$.

Fermat's (Little) Theorem

Theorem I

Given $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, such that $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem II

Given $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, then

$$a^{p} \equiv a \pmod{p}$$

Fermat's (Little) Theorem

Let us compute the remainder of 8^{103} when divided by 13 . Using Fermat's theorem, we have

$$\begin{aligned} 8^{103} &\equiv \left(8^{12}\right)^{8}\left(8^{7}\right) \equiv \left(1^{8}\right)\left(8^{7}\right) \equiv 8^{7} \equiv (-5)^{7} \\ &\equiv (25)^{3}(-5) \equiv (-1)^{3}(-5) \equiv 5 (\bmod 13) \end{aligned}$$

Exercise 5

Show that $2^{11,213} - 1$ is not divisible by 11 .

Exercise 5 Solution

By Fermat's theorem, $2^{10} \equiv 1(\bmod 11)$, so

$$
\begin{aligned}
2^{11,213} - 1 &\equiv \left[\left(2^{10}\right)^{1,121} \cdot 2^{3}\right] - 1 \equiv \left[1^{1,121} \cdot 2^{3}\right] - 1 \\
&\equiv 2^{3} - 1 \equiv 8 - 1 \equiv 7(\bmod 11)
\end{aligned}
$$

Euler's Theorem

Theorem

For $m \in \mathbb{N} \backslash \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

where $\varphi(m)$ is the number of invertible integers modulo m.

Euler's Theorem

1. Compute $\varphi\left(p^2\right)$ where p is a prime.
2. Compute $\varphi(pq)$ where both p and q are primes.

Euler's Theorem

1. All positive integers less than p^2 that are not divisible by p are relatively prime to p. Thus welete from the p^2-1 integers less than p^2 the integers $p, 2p, 3p, \cdots, (p-1)p$. There are $p-1$ integers deleted, so $\phi\left(p^2\right)=\left(p^2-1\right)-(p-1)=p^2-p$
2. We delete from the $pq-1$ integers less than pq those that are mltiples of p or of q to obtain those relatively prime to pq. The multiples of p are $p, 2p, 3p, \cdots, (q-1)p$ and the multiples of q are $q, 2q, 3q, \cdots, (p-1)q$. Thus we delete a total of $(q-1)+(p-1)=p+q-2$ elements, so $\phi(pq)=(pq-1)-(p+q+2)=pq-p-q+1=(p-1)(q-1)$.

Congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence. Such congruences arise throughout number theory and its applications.

How can we solve the linear congruence $ax \equiv b \pmod{m}$, that is, how can we find all integers x that satisfy this congruence? One method that we will describe uses an integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\bar{a}$ is said to be an inverse of a modulo m. Theorem 1 guarantees that an inverse of a modulo m exists whenever a and m are relatively prime.

Congruences

Let d be the gcd of positive integers a and m. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m.

Congruences

Find all solutions of the congruence $12x \equiv 27 (\mathrm{mod} 18)$.
Solution: The gcd of 12 and 18 is 6 , and 6 is not a divisor of 27.
Thus by the preceding theorem, there are no solutions.

Solving Congruences

What are the solutions of the linear congruence $101x \equiv 583 \pmod{4620}$?

Solving Congruences

1. The gcd of 101 and 4620 is 1 , and 1 is a divisor of 583. Thus by the preceding theorem, there is a solution.

Solving Congruences

2. Find an inverse of 101 modulo 4620.

The steps used by the Euclidean algorithm to find gcd(101, 4620) are

$$
\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

Solving Congruences

3. Because the last nonzero remainder is 1 , we know that $\gcd(101, 4620) = 1$. We can now express $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.
In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend. We obtain

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\
&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\
&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}
$$

Solving Congruences

4. 1601 is an inverse of 101 modulo 4620.

Solving Congruences

5. Multiplying both sides of the congruence by 1601 shows that $1601 \cdot 101x \equiv 1601 \cdot 583 (\mathrm{mod} 4620)$ Because $161701 \equiv 1 (\mathrm{mod} 4620)$ and $933383 \equiv 143 (\mathrm{mod} 4620)$, it follows that if x is a solution, then $x \equiv 143 (\mathrm{mod} 4620)$.

Solving Congruences

5. Multiplying both sides of the congruence by 1601 shows that $1601 \cdot 101x \equiv 1601 \cdot 583 (\mod 4620)$ Because $161701 \equiv 1 (\mod 4620)$ and $933383 \equiv 143 (\mod 4620)$, it follows that if x is a solution, then $x \equiv 143 (\mod 4620)$.

Fast Modular Exponentiation

In cryptography it is important to be able to find $b^n \bmod m$ efficiently, where b, n, and m are large integers. It is impractical to first compute b^n and then find its remainder when divided by m because b^n will be a huge number. Instead, we can use an algorithm that employs the binary expansion of the exponent n. Before we present this algorithm, we illustrate its basic idea. We will explain how to use the binary expansion of n, say $n = (a_{k-1} \ldots a_1 a_0)_2$, to compute b^n. First, note that

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1\cdot 2} \cdot b^{a_0}$$

Fast Modular Exponentiation

This shows that to compute b^n, we need only compute the values of $b, b^2, \left(b^2\right)^2 = b^4, \left(b^4\right)^2 = b^8, \ldots, b^{2^k}$. Once we have these values, we multiply the terms b^{2^j} in this list, where $a_j = 1$. (For efficiency, after multiplying by each term, we reduce the result modulo m.) This gives us b^n. For example, to compute 3^{11} we first note that $11 = (1011)_2$, so that $3^{11} = 3^8 3^2 3^1$. By successively squaring, we find that $3^2 = 9, 3^4 = 9^2 = 81$, and $3^8 = (81)^2 = 6561$. Consequently, $3^{11} = 3^8 3^2 3^1 = 6561 \cdot 9 \cdot 3 = 177,147$.

The algorithm successively finds $b \bmod m, b^2 \bmod m, b^4 \bmod m, \ldots, b^{2^{k-1}} \bmod m$ and multiplies together those terms $b^{2^j} \bmod m$ where $a_j = 1$, finding the remainder of the product when divided by m after each multiplication.

Example

$$2^{2021} \bmod 2021$$

Example

Consider $2^{2021} \bmod 2021$. We first note that the binary representation of 2021 is

$$2021 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2^0.$$

Then we know that $2^{2021} = 2^{2^{10}+2^9+2^8+2^7+2^6+2^5+2^2+2^0} = 2^{2^{10}} \times 2^{2^9} \times 2^{2^8} \times 2^{2^7} \times 2^{2^6} \times 2^{2^5} \times 2^{2^2} \times 2^{2^0}$

Example

Calculating that

$$
\begin{aligned}
2^{1} &\equiv 2 \bmod 2021 \\
2^{2^2} &\equiv 16 \bmod 2021 \\
2^{2^5} &\equiv 747 \bmod 2021 \\
2^{2^6} &\equiv 213 \bmod 2021 \\
2^{2^7} &\equiv 907 \bmod 2021 \\
2^{2^8} &\equiv 102 \bmod 2021 \\
2^{2^9} &\equiv 299 \bmod 2021 \\
2^{2^{10}} &\equiv 477 \bmod 2021
\end{aligned}
$$

$$2^{2021} \equiv 477 \times 299 \times 102 \times 907 \times 213 \times 747 \times 16 \times 2 \equiv 1322 \bmod 2021$$

Chinese Remainder Theorem

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?

Find x such that

$$x \equiv 2(\bmod 3)$$
$$x \equiv 3(\bmod 5)$$
$$x \equiv 2(\bmod 7)$$

三人同行七十希，五树梅花廿一支，七子团圆正半月，除百零五便得知。

$$x \equiv 2 \times 70 + 3 \times 21 + 2 \times 15 = 233 \equiv 23(\bmod 105)$$

$$70 \equiv 1(\bmod 3), 70 \equiv 0(\bmod 5), 70 \equiv 0(\bmod 7)$$
$$21 \equiv 0(\bmod 3), 21 \equiv 1(\bmod 5), 21 \equiv 0(\bmod 7)$$
$$15 \equiv 0(\bmod 3), 15 \equiv 0(\bmod 5), 15 \equiv 1(\bmod 7)$$
$$105 \equiv 0(\bmod 3), 105 \equiv 0(\bmod 5), 105 \equiv 0(\bmod 7)$$

Chinese Remainder Theorem

Solve the following system of linear congruence

$$x \equiv 3 \pmod{8}$$
$$x \equiv 1 \pmod{15}$$
$$x \equiv 11 \pmod{20}$$

Chinese Remainder Theorem

Solution: Note that by Chinese remainder's theorem, the original system is equivalent to

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 11 \pmod{4} \\ x &\equiv 11 \pmod{5} \end{aligned}$$

Note that (1) implies (4), and (3) and (5) are the same, hence the original system is equivalent to

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{3} \end{aligned}$$

Chinese Remainder Theorem

where the moduli are pairwise coprime. Note that last two implies that $x \equiv 1 \pmod{15}$, we therefore can reduced the system above into

$$x \equiv 3 \pmod 8$$
$$x \equiv 1 \pmod{15}$$

Let $x = 15y + 1 = 8z + 3$, thus $15y - 8z = 2$. By inspection, we have $(15)(1) - (8)(2) = -1$, thus we can choose $y = -2$ and $z = -4$ such that $15y - 8z = 2$. Now $x = 15y + 1 = -29$. Therefore the solution to the original system of Diophantine equation is given by

$$x \equiv -29 \pmod{120}$$

Exercise 6

Solve the following system of linear congruence

$$
\begin{aligned}
x &\equiv 6 \pmod{11} \\
x &\equiv 13 \pmod{16} \\
x &\equiv 9 \pmod{21} \\
x &\equiv 19 \pmod{25}
\end{aligned}
$$

Exercise 6 Solution

Solution: Since $11, 16, 21$, and 25 are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m, where $m = 11 \cdot 16 \cdot 21 \cdot 25 = 92400$.
We apply the technique of the Chinese Remainder Theorem with

$$k = 4, \quad m_1 = 11, \quad m_2 = 16, \quad m_3 = 21, \quad m_4 = 25,$$

$$a_1 = 6, \quad a_2 = 13, \quad a_3 = 9, \quad a_4 = 19,$$

to obtain the solution.

Exercise 6 Solution

We compute

$$z_1 = m/m_1 = m_2 m_3 m_4 = 16 \cdot 21 \cdot 25 = 8400$$
$$z_2 = m/m_2 = m_1 m_3 m_4 = 11 \cdot 21 \cdot 25 = 5775$$
$$z_3 = m/m_3 = m_1 m_2 m_4 = 11 \cdot 16 \cdot 25 = 4400$$
$$z_4 = m/m_4 = m_1 m_3 m_3 = 11 \cdot 16 \cdot 21 = 3696$$
$$y_1 \equiv z_1^{-1} \pmod{m_1} \equiv 8400^{-1} \pmod{11} \equiv 7^{-1} \pmod{11} \equiv 8 \pmod{11}$$
$$y_2 \equiv z_2^{-1} \pmod{m_2} \equiv 5775^{-1} \pmod{16} \equiv 15^{-1} \pmod{16} \equiv 15 \pmod{16}$$
$$y_3 \equiv z_3^{-1} \pmod{m_3} \equiv 4400^{-1} \pmod{21} \equiv 11^{-1} \pmod{21} \equiv 2 \pmod{21}$$
$$y_4 \equiv z_4^{-1} \pmod{m_4} \equiv 3696^{-1} \pmod{25} \equiv 21^{-1} \pmod{25} \equiv 6 \pmod{25}$$
$$w_1 \equiv y_1 z_1 \pmod{m} \equiv 8 \cdot 8400 \pmod{92400} \equiv 67200 \pmod{92400}$$
$$w_2 \equiv y_2 z_2 \pmod{m} \equiv 15 \cdot 5775 \pmod{92400} \equiv 86625 \pmod{92400}$$
$$w_3 \equiv y_3 z_3 \pmod{m} \equiv 2 \cdot 4400 \pmod{92400} \equiv 8800 \pmod{92400}$$
$$w_4 \equiv y_4 z_4 \pmod{m} \equiv 6 \cdot 3696 \pmod{92400} \equiv 22176 \pmod{92400}$$

Exercise 6 Solution

The solution, which is unique modulo 92400 , is

$$
\begin{aligned}
x &\equiv a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod{92400} \\
&\equiv 6 \cdot 67200 + 13 \cdot 86625 + 9 \cdot 8800 + 19 \cdot 22176 \pmod{92400} \\
&\equiv 2029869 \pmod{92400} \\
&\equiv \mathbf{51669} \pmod{92400}
\end{aligned}
$$

1. Ring (Optional)

2. Modular Arithmetic
   - Modulo
   - Fermat's (Little) Theorem
   - Congruences
   - Fast Modular Exponentiation
   - Chinese Remainder Theorem
   - RSA Cryptography

3. Q&A

RSA Cryptography

Goal: Transfer information from A (Alice) to B (Bob).
Trapdoor Function: Want to find a (bijective) trapdoor function $f : S \to S, S$ a HUGE set, such that
- Easy to compute.
- HARD to invert.
- Unless one has the secret key.

RSA Cryptography

1. (Alice) Choose 2 (large) distinct primes, e.g., $p = 17, q = 19$.
2. (Alice) Let $n = pq = 17 \times 19 = 323$.
3. (Alice) Let $A = \varphi(n) = (p-1)(q-1) = 16 \times 18 = 288$. (Keep private!)
4. (Alice) Pick[4] $E < \varphi(n)$ such that $\gcd(E, \varphi(n)) = 1$, say, $E = 95$. Publish public key $(n, E) = (323, 95)$, with (public) encryption function e (for Bob)

$$y = e(x) = x^E (\bmod n), \quad \text{e.g., } y = e(x) = x^{95} (\bmod 323)$$

5. (Alice) Compute private key, $D = E^{-1} (\bmod A)$. Then the decryption function d is given by

$$d(y) = y^D = x^{ED} \equiv x (\bmod n), \quad \text{e.g., } d(y) = y^{191} (\bmod 323)$$

Exercise 7

In an RSA procedure, the public key is chosen as $(n, E) = (2077, 97)$, i.e., the encryption function e is given by

$$e(x) = x^{97} \pmod{2077}$$

(Note that $2077 = 31 \times 67$.)
Compute the private key D, where $D = E^{-1} (\bmod \varphi(n))$. Decrypt the message 279 , that is, find x if $y = e(x) = 279 (\bmod 2077)$.

Exercise 7 Solution

Note that $\varphi(2077) = (31-1)(67-1) = 1980$. We need to solve $97D \equiv 1 \pmod{1980}$. By Euclidean algorithm (or anything else that works)

$$\begin{aligned}
1980 &= 97 \times 20 + 40 \\
97 &= 40 \times 2 + 17 \\
40 &= 17 \times 2 + 6 \\
17 &= 6 \times 2 + 5 \\
6 &= 5 \times 1 + 1
\end{aligned}$$

Exercise 7 Solution

hence

$$
\begin{aligned}
1 &= 6 - 5 \\
&= 6 - (17 - 6 \times 2) = 6 \times 3 - 17 \\
&= (40 - 17 \times 2) \times 3 - 17 = 40 \times 3 - 17 \times 7 \\
&= 40 \times 3 - (97 - 40 \times 2) \times 7 = 40 \times 17 - 97 \times 7 \\
&= (1980 - 97 \times 20) \times 17 - 97 \times 7 \\
&= 1980 \times 17 - 97 \times 347
\end{aligned}
$$

Thus $D \equiv -347 \equiv 1633 (\bmod 1980)$.

Exercise 7 Solution

We need to calculate $279^D (\bmod 2077)$. First note that

$$1633 = (11001100001)_2 = 2^{10} + 2^9 + 2^6 + 2^5 + 2^0$$

Then

Exercise 7 Solution

$$279^{2^0} \equiv 279 \pmod{2077}$$
$$279^{2^1} \equiv 279^2 \equiv 992 \pmod{2077}$$
$$279^{2^2} \equiv 992^2 \equiv -434 \pmod{2077}$$
$$279^{2^3} \equiv (-434)^2 \equiv -651 \pmod{2077}$$
$$279^{2^4} \equiv (1426)^2 \equiv 93 \pmod{2077}$$
$$279^{2^5} \equiv 93^2 \equiv 341 \pmod{2077}$$
$$279^{2^6} \equiv 341^2 \equiv (-31) \pmod{2077}$$
$$279^{2^7} \equiv (-31)^2 \equiv 961 \pmod{2077}$$
$$279^{2^8} \equiv 961^2 \equiv 1333 \pmod{2077}$$
$$279^{2^9} \equiv 1333^2 \equiv 1054 \pmod{2077}$$
$$279^{2^{10}} \equiv 1054^2 \equiv -279 \pmod{2077}$$

Exercise 7 Solution

Hence

$$
\begin{aligned}
279^{1871} &\equiv 279^{2^0} + 2^5 + 2^6 + 2^9 + 2^{10} \\
&\equiv 279^{2^0} \cdot 279^{2^5} \cdot 279^{2^6} \cdot 279^{2^9} \cdot 279^{2^{10}} \\
&\equiv (279)(341)(-31)(1054)(-279) \\
&\equiv (-403)(-31)(1054)(-279) \\
&\equiv (31)(1054)(-279) \\
&\equiv (-558)(-279) \\
&\equiv 1984 \pmod{2077}
\end{aligned}
$$

1. Ring (Optional)
2. Modular Arithmetic
   - Modulo
   - Fermat's (Little) Theorem
   - Congruences
   - Fast Modular Exponentiation
   - Chinese Remainder Theorem
   - RSA Cryptography
3. Q&A

Q&A

Q&A