Hw2

Nmae: Wei Jun Li
Rin: 662006326

February 25, 2024

1 problem 1

1.1 85871 mod 67

formual: $ab = ((a\%x)(b\%x)\%x)$

So we have:
85871 % 67 == ((43% 67) (1997 %67)%67)
== ((43 * 53)% 67)
== 2322 % 67
== 44

1.2 5 mod -11

formual: $a = qn + b$

So we have:
5 = -11 * q + b
q = -1
so we get the result: 5 == 11 + b => b = -6
The anwer we get is 5 mod -11 is equal to -6

1.3 -149 mod 19

formual: $a = qn + b$

So we have:
-149 = 19 * q + b
q = -8
so we get the result: -149 == -152 + b => b = 3
The anwer we get is -149 mod 19 is equal to 3

2 problem 2

2.1 $17^{30} \mod 31$

We aim to calculate $17^{30} \mod 31$. By Fermat's Little Theorem, if p is a prime number, and a is a positive integer less than p and co-prime to p, then $a^{p-1} \equiv 1 \mod p$.

Since 31 is a prime number and 17 is less than 31, we can assert:

$$17^{30} \equiv 1 \mod 31$$

This is because:

$$\begin{aligned} gcd(17, 31) &= 1 \quad \text{(17 and 31 are co-prime)} \\ 17^{31-1} &= 17^{30} \\ 17^{30} \mod 31 &= 1 \end{aligned}$$

Therefore, we can conclude that $17^{30} \mod 31 = 1$ directly, without the need for extensive calculation.

2.2 $53^{1069} \mod 54$

As we know that:

$$\begin{aligned} 53 &\equiv -1 \mod 54 \\ 53^{1069} \mod 54 &= (-1)^{1069} \mod 54 \\ &= -1 \mod 54 \\ &= 53 \end{aligned}$$

Furthermore, for any odd exponent n:

$$\begin{aligned} (-1)^n \mod d &= (-1) \mod d \\ 53^{1069} \mod 54 &= (-1)^{1069} \mod 54 \\ &= (-1) \cdot 1 \mod 54 \\ &= 53^1 \mod 54 \\ &= 53 \end{aligned}$$

Therefore, $53^{1069} \mod 54 = 53$.

3 problem 3

3.1 $13^{-1} \mod 101$

To find the modular inverse of 13 modulo 101, we seek an integer x such that $13x \equiv 1 \mod 101$. This problem is equivalent to finding x and y that satisfy $13x + 101y = 1$, which can be solved using the Extended Euclidean Algorithm.

Extended Euclidean Algorithm

The algorithm finds integers x and y such that $ax+by = \gcd(a, b)$. For our case, $a = 13$ and $b = 101$, and we apply the algorithm to compute x in $13x + 101y = \gcd(13, 101)$.

Solution

By applying the Extended Euclidean Algorithm, we initially obtain $x = -31$, which is the coefficient of 13 in the Bézout's identity. However, since we require a positive solution within the modular system, we calculate $x \mod 101$, yielding $x = 70$.

Therefore, the modular inverse of 13 modulo 101 is 70, which can be formally written as $13^{-1} \mod 101 = 70$.

3.2 $1234^{-1} \mod 4321$

To find the modular inverse of 1234 modulo 4321, we need to solve for x in the congruence $1234x \equiv 1 \mod 4321$. This can be transformed into finding x and y that satisfy $1234x + 4321y = 1$, which is a linear Diophantine equation. The Extended Euclidean Algorithm provides a way to find such x and y.

Extended Euclidean Algorithm

The algorithm is based on the principle that $\gcd(a, b)$ can be expressed as $ax+by$, where x and y are integers. For our case, we apply the algorithm to find x in the equation $1234x + 4321y = \gcd(1234, 4321)$.

Initially, we compute $\gcd(1234, 4321)$, which is 1, indicating that 1234 and 4321 are coprime and an inverse exists. The steps are as follows:

1. Apply the algorithm recursively until $a = 0$. In our base case, we return $b = \gcd(a, b)$, $x = 0$, and $y = 1$.

2. For each recursive step, calculate $b \mod a$, and update x and y based on the recursion: $x = y - \left\lfloor \frac{b}{a} \right\rfloor \cdot x$, $y = x$.

Solution

Through the Extended Euclidean Algorithm, we find that the modular inverse of 1234 modulo 4321 is x, where x is adjusted to be positive by taking $x \mod 4321$.

Calculation

The specific calculation yields $x = -1082$, but since we require a positive integer in the range of 0 to 4320 (inclusive), we adjust x by computing $x \mod 4321$, resulting in $x = 3239$.

Therefore, the modular inverse of 1234 modulo 4321 is 3239.

4 Problem 4

4.1 $(\frac{x^3+1}{x+1}) \mod (x^3 + x^2 + 1)$

Given a polynomial division in $GF(2^n)$, we aim to calculate $(\frac{x^3+1}{x+1})$ and then find its modulo over $(x^3 + x^2 + 1)$. In $GF(2^n)$, polynomial arithmetic follows unique rules where addition is equivalent to the XOR operation, and multiplication follows polynomial multiplication rules modulo a reducing polynomial, which, in this case, is not required since the division and modulo operation do not increase the polynomial degree.

Calculation

$$\frac{x^3 + 1}{x + 1} = x^2 + x + 1$$

As per the arithmetic in $GF(2^n)$, the division yields a polynomial of x^2+x+1, which is already in its simplest form and does not require further reduction by the modulus $(x^3 + x^2 + 1)$.

Therefore, the result of $(\frac{x^3+1}{x+1} \mod (x^3 + x^2 + 1)) = x^2 + x + 1$.

4.2 $(x^8 + x^4 + x^2 + x + 1) \mod (x^6 + x + 1)$

Given the polynomial $f(x) = x^8+x^4+x^2+x+1$ and the modulus $g(x) = x^6+x+1$ in $GF(2^n)$, we aim to find $f(x) \mod g(x)$.

Polynomial Division

To perform the division $f(x) \div g(x)$, we need to align the highest degree term of $g(x)$ with that of $f(x)$ by multiplying $g(x)$ by an appropriate monomial. The process involves multiple steps, where in each step, we subtract (in $GF(2^n)$, subtraction is the same as addition) the product from $f(x)$ to get the remainder. This process is repeated until the degree of the remainder is less than the degree of $g(x)$.

Steps

1. Multiply $g(x)$ by x^2 to match the highest degree term of $f(x)$, resulting in $x^8 + x^3 + x^2$. Subtract this from $f(x)$ to get the new remainder $r_1(x) = x^4 + x^3 + x + 1$.

2. For the next step, notice that the highest degree term of the new remainder $r_1(x)$ is x^4, which is lower than the degree of $g(x)$, thus stopping the division process.

Result

Therefore, the remainder of $f(x) \div g(x)$ in $GF(2^n)$ is $r_1(x) = x^4 + x^3 + x + 1$, which means $f(x) \mod g(x) = x^4 + x^3 + x + 1$.

5 Problem 5

Use Fermat's theorem to find:

5.1 $3^{201} \mod 11$

Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$. This theorem can be used to compute large exponents modulo a prime number efficiently.

Calculation of $3^{201} \mod 11$

Given that 11 is a prime number and using Fermat's Little Theorem, we know that:

$$3^{10} \equiv 1 \mod 11$$

For any integer a, and k being a multiple of 10, the exponent can be broken down as:

$$\begin{aligned} a^{k+1} &= a^k \cdot a \\ &= (a^{10})^{\frac{k}{10}} \cdot a \end{aligned}$$

Applying this to our case with $a = 3$ and $k = 200$, we get:

$$\begin{aligned} 3^{201} &= (3^{10})^{20} \cdot 3 \\ &\equiv 1^{20} \cdot 3 \mod 11 \\ &\equiv 3 \mod 11 \end{aligned}$$

Thus, by Fermat's Little Theorem, we conclude that:

$$3^{201} \mod 11 = 3$$

5.2 a number x between 0 and 28 where $x^{85} \mod 29 = 6$.

We want to find a number x between 0 and 28 such that $x^{85} \mod 29 = 6$. Fermat's Little Theorem tells us that if p is a prime number and a is an integer that is not divisible by p, then $a^{p-1} \equiv 1 \mod p$.

Since 29 is a prime number, by Fermat's Little Theorem, for any x not divisible by 29:

$$x^{28} \equiv 1 \mod 29$$

The exponent 85 can be written as $3 \times 28 + 1$, so x^{85} can be expressed as:

$$\begin{aligned}
x^{85} &= x^{84} \times x \\
&= (x^{28})^3 \times x \\
&\equiv 1^3 \times x \mod 29 \\
&\equiv x \mod 29
\end{aligned}$$

Given that $x^{85} \equiv 6 \mod 29$, we can deduce that:

$$x \equiv 6 \mod 29$$

Conclusion

Therefore, the number x that satisfies $x^{85} \mod 29 = 6$ is 6, which is within the range from 0 to 28.

In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?

Given the RSA encryption where the ciphertext C is 10, the public key exponent e is 5, and the modulus n is 35, the goal is to find the plaintext message M.

RSA Decryption

The RSA decryption requires finding the private key d, which is the modular multiplicative inverse of e modulo $\phi(n)$, where $\phi(n)$ is the Euler's totient function of n.

Since $n = 35$ and it is the product of two primes $p = 5$ and $q = 7$, we have:

$$\begin{aligned} \phi(n) &= (p-1)(q-1) \\ &= (5-1)(7-1) \\ &= 4 \cdot 6 \\ &= 24 \end{aligned}$$

The private key d satisfies the congruence:

$$\begin{aligned} ed &\equiv 1 \mod \phi(n) \\ 5d &\equiv 1 \mod 24 \end{aligned}$$

Using the modular inverse function, we find that $d = 5$.
The plaintext message M is then found using the following congruence:

$$\begin{aligned} M &\equiv C^d \mod n \\ &\equiv 10^5 \mod 35 \end{aligned}$$

Upon calculation, we determine that the plaintext message $M = 5$.