**G01501801**

**SRI TEJA KALE**

**HOMEWORK 2**

**1. In mod n arithmetic why does x have a multiplicative inverse if and only if x is relatively prime to n? (10 points)**

* In modular arithmetic, specifically modulo *n*, an element *x* is said to have a multiplicative inverse if there exists an integer *y* such that:

*(x · y) ≡ 1 (mod n)*

* This equation means that when *x* is multiplied by *y*, the result is congruent to 1 modulo *n*. Now, the existence of such a *y* depends entirely on the relationship between *x* and *n*.
* If x is relatively prime to n (i.e., gcd(x, n) = 1), then x has a multiplicative inverse modulo n.
* This is true because when the greatest common divisor (gcd) of *x* and *n* is 1, Bézout’s Identity tells us that there exist integers *a* and *b* such that:

*a·x + b·n = 1*

* Rewriting this modulo *n*, the term *b·n* becomes congruent to 0, so we get:

*a·x ≡ 1 (mod n)*

* This shows that *a* is the multiplicative inverse of *x* modulo *n*. Therefore, a multiplicative inverse exists only when *x* and *n* are coprime.
* If x has a multiplicative inverse modulo n, then x is relatively prime to n.
* Suppose *x* does have a multiplicative inverse modulo *n*. That means there exists some *y* such that:

*x·y ≡ 1 (mod n)*  
⟹ *x·y - 1 ≡ 0 (mod n)*  
⟹ *x·y - 1* is divisible by *n*

This implies:

*x·y + n·(-k) = 1* for some integer *k*

* Again, this is Bézout’s Identity in action, showing that a linear combination of *x* and *n* equals 1. Therefore, the greatest common divisor of *x* and *n* must be 1.
* Hence, the existence of a multiplicative inverse modulo *n* is equivalent to the condition that *x* is relatively prime to *n*. This is because only when *x* and *n* share no common divisors other than 1 can a linear combination of them equal 1, which is precisely the condition required for a multiplicative inverse to exist under modulo *n* arithmetic.

**2. What is the probability that a random chosen number would not be relatively prime to some particular RSA modulus n=p\*q? What threat would finding such a number pose? (10 points)**

An RSA modulus n is the product of two large prime numbers, p and q. A number a chosen randomly from the set {1,2,...,n−1} is not relatively prime to n if and only if it shares a nontrivial common factor with n, i.e., gcd(a,n)≠1.

Now, since n=p⋅q, the only positive integers less than n that are not relatively prime to n must be multiples of either p or q.

Let’s calculate the number of integers in {1,2,...,n−1} that are not relatively prime to n.

* There are ⌊n−1/p⌋ multiples of p less than n, and similarly ⌊n−1/q⌋ multiples of q.
* However, numbers that are multiples of both p and q (i.e., multiples of pq=n) are rare.In fact, there’s only one such number less than or equal to n−1, and that’s 0, which is excluded from our range.

So, the number of integers less than n that are not relatively prime to n is approximately:

⌊n/p⌋+⌊n/q⌋−1≈n/p + n/q−1

Since p and q are large primes (often 1024 bits each), this number is extremely small relative to n. Therefore, the probability that a randomly chosen number is not relatively prime to n is:

P(gcd(a,n)≠1)≈1/p+1/q

Given that p and q are large (say, on the order of 2^{512}), this probability is negligible , practically zero.

Threat Posed:

Despite the low probability, finding such a number poses a serious threat to RSA security:

* If an attacker finds a number aa such that gcd(a,n)≠1, then gcd(a,n) must be either p or q, since these are the only prime factors of n.
* Computing the greatest common divisor is extremely efficient (via the Euclidean algorithm).
* If either p or q is discovered, the RSA modulus n can be factored easily, breaking the encryption system.
* Once p and q are known, an attacker can compute the private key and decrypt any ciphertext or forge signatures.

In short, even one such number can completely compromise the RSA cryptosystem.

Hence, the probability of randomly selecting a number that is not relatively prime to an RSA modulus n=p⋅q is negligibly small, roughly 1/p+1/q. However, finding such a number is extremely dangerous, as it leads directly to the factorization of n, ultimately breaking RSA security.

**3. If a and b are relatively prime, and bc is a multiple of a, show that c is a multiple of a. (10 points) [Hint” use the result of Euclid’s algorithm**

We are given that a and b are relatively prime, and that bc is a multiple of a. Our goal is to demonstrate that c must be a multiple of a.

**Step 1: Use the fact that a and b are relatively prime**

* Since gcd(a,b)=1, there exist integers x and y such that:

ax+by=1

* This is a result of Euclid's algorithm, which expresses 1 as a linear combination of a and b.

**Step 2: Multiply the equation by c**

* Now, multiply both sides of the equation ax+by=1 by c:

c(ax+by)=c

* Expanding this gives:

acx+bcy=c

* Since we are given that bc=ak for some integer k (because bc is a multiple of a), we can substitute bc with ak in the above equation:

acx+aky=c

* Now, factor out a from the first two terms:

a(cx+ky)=c

At this point, it's clear that c is divisible by a, since the right-hand side is a multiple of a. Hence, c must be a multiple of a.

Hence, we have shown that if a and b are relatively prime and bc is a multiple of a, then c must also be a multiple of a.

**4. Calculate the following (20 points)**

**φ(18) (4 points)**

* Euler’s Totient Function ϕ(n)counts the number of integers between 1 and n that are relatively prime to n. To calculate ϕ(18), we first find the prime factorization of 18:

18=2×32

* Now, using the formula for the totient function:

ϕ(n)=n(1−1/p1) (1−1/p2) …(1−1/pk)

* where n = p1e1 p2e2 is the prime factorization of n. Applying this to 18=2×32:

ϕ(18)=18(1−1/2)(1−1/3)

ϕ(18)=18×1/2×2/3

ϕ(18)=18×1/3=6

So, ϕ(18)=6.

**105363 mod 91 (8 points)**

**Step 1: Simplify the Base Modulo 91**

First, I need to simplify the base, 105, modulo 91.

105÷91=1 with a remainder of 14

So,

105≡14mod 91

**Step 2: Apply Euler's Theorem**

Euler's theorem states that if two numbers, a and *n*, are coprime, then:

aϕ(n)≡1mod n

Where ϕ(n) is Euler's totient function.

First, check if 14 and 91 are coprime.

The prime factors of 91 are 7 and 13.

The prime factors of 14 are 2 and 7.

Since both share a common factor of 7, they are not coprime. Therefore, Euler's theorem does not apply directly.

**Step 3: Simplify the Exponent Using Euler's Totient Function**

Even though Euler's theorem doesn't apply directly, I can still use the concept to simplify the exponent.

Calculate ϕ(91):

ϕ(91)=91×(1−1/7)×(1−1/13)=91×6/7×12/13=72.

So, ϕ(91)=72*.*

**Step 4: Reduce the Exponent Modulo ϕ(91)**

363÷72=5 with a remainder of 3

So,

363≡3mod 72

Therefore,

105363≡143mod 91

**Step 5: Calculate 143mod 91**

143=14×14×14=2744

Now, find 2744mod 91:

2744÷91=30 with a remainder of 14

So,

2744≡14mod 91

105363≡14mod 91

Hence, 105363mod 91=14

**204994 mod 287 (8 points)**

**Step 1: Simplify the Base Modulo 287**

First, simplify 204 modulo 287.

204÷287=0 with a remainder of 204

So,

204≡204mod 287

**Step 2: Apply Euler's Theorem**

Check if 204 and 287 are coprime.

Prime factors of 287: 7 and 41.

Prime factors of 204: 2, 3, and 17.

Since they share no common prime factors, they are coprime. Therefore, Euler's theorem applies.

**Step 3: Calculate Euler's Totient Function ϕ(287)**

ϕ(287)=287×(1−1/7)×(1−1/41)=287×6/7×40/41=240.

So, ϕ(287)=240.

**Step 4: Reduce the Exponent Modulo ϕ(287)**

994÷240=4 with a remainder of 34

So,

994≡34mod 240

Therefore,

**204994≡20434mod 287**

**Step 5: Simplify 20434mod 287 Using Successive Squaring**

Calculating 20434directly is challenging, so I'll use the method of successive squaring.

First, express 34 in binary to determine the powers needed:

34=32+2=25+21

So, I need to compute 20432 and 2042, then multiply them together modulo 287.

**Compute 2042mod 287:**

2042=41616

41616÷287=145 with a remainder of 1

So,

2042≡1mod 287

**Compute 20432mod 287:**

Since 2042≡1mod 287, then:

20432=(2042)16≡116≡1mod  287

**Multiply the Results:**

20434=20432×2042≡1×1≡1mod 287

204994≡1mod 287

**Hence, 204994mod287=1**