CS 3510 — Algorithms, Spring 2022

Homework 1C Solutions

Modular Arithmetic

Part A One way of defining congruence modulo n is as follows: given integers $x, y, n > 0$ we say that $x \equiv y \mod n$ when $x = y + cn$ (with $c \in \mathbb{Z}$). Prove if that if $x \equiv x' \mod n$ then any polynomial function with integer coefficients f, we have $f(x) \equiv f(x') \mod n$.

Proof. Any polynomial f with integer coefficients can be represented as:

$$f(x) = \sum a_i x^i$$

where $a_i \in \mathbb{Z}$. With this in mind, we also know that since $x \equiv x' \mod n$, then $x = x' + cn$. Therefore, in the above function, it is equivelant to plug in $x' + cn$ for x:

$$\begin{aligned} f(x) &= \sum a_i x^i \\ &= \sum a_i (x' + cn)^i \end{aligned}$$

By the Binomial Theorem for expanding polynomial, every term except one in the expansion of $(x' + cn)^i$ will contain some product of cn meaning that all these terms will be divisible by n.

The only term that will not be divisible by n would be $(x')^n$. But, under modulo n, since all the other terms are divisible by n, they are 0 in this congruence.

Therefore:

$$f(x) = \sum a_i x^i = \sum a_i (x' + cn)^i \equiv_N \sum a_i (x')^i = f(x') \mod n$$

□

Part B Solve for x in each of the following modular exponentiation questions.

1. $27^{43} \equiv x \mod 127$

   Solution: Notice that 27 is a perfect cube and can be written as 3^3, then $27^{43} = \left(3^3\right)^{43} = 3^{129}$.

   By Little Fermat's, we know that $a^{126} \equiv 1 \mod 127$ since 127 is prime. Therefore, $3^{126} \equiv 1 \mod 127$.

   Using this fact, we can manipulate 3^{129} as $3^3 3^{126}$.

   $$\begin{aligned} 3^{129} &\equiv_{127} x \\ 3^3 3^{126} &\equiv_{127} x \\ 3^3 &\equiv_{127} x \\ 27 &\equiv_{127} x \end{aligned}$$

   Hence, $\boxed{x = 27}$.

2. $2^{2n} \equiv x \mod 3$

   Solution: $2 \equiv_3 -1$ therefore this is equivelant to $(-1)^{2n}$ and -1 raised to any even power is 1, therefore $\boxed{x = 1}$.

3. $5^8 \equiv x \mod 13$

   Solution: We can use modular exponentiation. Let $8 = 1000$, then we can compute $5, 5^2, 5^4, 5^8$ all under modulo 13 to get the answer.

   $$\begin{aligned} 5 &\equiv_{13} 5 \\ 5^2 = 25 &\equiv_{13} 12 \\ 5^4 \equiv_{13} 144 &\equiv_{13} 1 \\ 5^8 &\equiv_{13} 1 \end{aligned}$$

   Hence, $\boxed{x = 1}$.

Part C Use the Extended Euclidean algorithm to find a pair of integers x and y satisfying $57x - 91y = 1$ if such a pair exists.

Solution: We can continue by solving for $\gcd(91, 57)$ and then negating the coefficient we get from $57x + 91y = 1$ (prevents working with negative numbers):

$$\begin{aligned} 91 &= 1(57) + 34 \quad \rightarrow \quad 34 = 91 - 57 \\ 57 &= 1(34) + 23 \quad \rightarrow \quad 23 = 57 - 34 \\ 34 &= 1(23) + 11 \quad \rightarrow \quad 11 = 34 - 23 \\ 23 &= 2(11) + 1 \quad \rightarrow \quad 1 = 23 - 2(11) \end{aligned}$$

Hence, we can now construct from the equations on the right side:

$$\begin{aligned} 1 &= 23 - 2(11) \\ &= 23 - 2(34 - 23) = 23 - 2(34) + 2(23) = 3(23) - 2(34) \\ &= 3(57 - 34) - 2(34) = 3(57) - 3(34) - 2(34) = 3(57) - 5(34) \\ &= 3(57) - 5(91 - 57) = 3(57) - 5(91) + 5(57) = 8(57) - 5(91) \end{aligned}$$

Hence, we have found coefficients x, y such that $1 = 57x + 91y$. Those coefficients are $x = 8, y = -5$. To get the coefficients for $1 = 57x - 91y$ instead, we can simply negate y to get $\boxed{x = 8, y = 5}$.

Part D Prove or disprove the following statement:

$$x^y \equiv x^{y'} \text{ if } y \equiv y' \mod n$$

Proof. This statement is not true, let $x = 2, y = 3, n = 3$. Then $y' = 0$ but $2^3 = 8 \neq = 1 = 2^0$. Hence, this statement is not true. □

RSA Cryptosystem

Part A Suppose Alice wants to send Bob a message using the RSA scheme.

1. Who should generate the RSA keys?

   Solution: Since Bob will need to be able to decrypt the message, he should have the private key which means he needs to generate the keypair and send the public key to Alice so that Alice can encrypt her message.

2. Suppose the person generating the key chooses the primes $p = 13$, $q = 29$ and the encryption exponent $e = 5$. What must the decryption exponent d be?

   Solution: Since $p = 13, q = 29$, then $(p-1)(q-1) = 12 \cdot 28 = 336$. Hence, we want to find the multiplicative inverse of $5 \mod 336$:

   $$336 = 67(5) + 1 \quad \rightarrow \quad 1 = 336 - 67(5)$$

   The coefficient in the above equation for 5 is -67 which means this is a multiplicative inverse. In the context of an exponent, this does not make much sense, so we can also add 336 to it to get a value of $\boxed{269}$.

   Remark: Both solutions are valid.

3. If the message being sent is $m = 6$, then what is the encrypted message?

   Solution: Since the encryption exponent is 5, we compute $6^5 = 7776$ and $N = pq = 29 \cdot 13 = 377$. Using a calculator, we know $7776 \mod 377 = 236$ which is the encrypted message that Alice can share with Bob.

Part B Why is a small encryption exponent sometimes problematic? Especially when the message is short?

Solution: Since P and Q can be very large numbers, $N = PQ$ is also a large number. Hence, if we have a small message and are raising it to a small exponent, it is highly probably that m^e is not greater than N.

Further, since e is public and there is a high probability of m^e not being modded by N, we can simply compute the e^{th} (5th in this case) to get the original message, making this encryption fairly weak.

Fermat's Primarlity Test

```
def naiveIsPrime(N, k):
    for i = 1 to k:
        x = a integer in the range [2, N-1]
        if (x^(n-1) % n) != 1:
            return false
    return true
```

1. What is the probability that `naiveIsPrime(13, 1)` returns true?

   Solution: Since 13 is prime, the probability of this event is 1 or 100%.

2. What is the probability that `naiveIsPrime(9, 1)` returns true?

   Solution: 9 is not prime, so we need to check how many numbers from $2 \to 8$ are bad:

$$
\begin{aligned}
x = 2: &\quad 2^8 \mod 9 \equiv 4 \to false \\
x = 3: &\quad 3^8 \mod 9 \equiv 0 \to false \\
x = 4: &\quad 4^8 \mod 9 \equiv 7 \to false \\
x = 5: &\quad 5^8 \mod 9 \equiv 7 \to false \\
x = 6: &\quad 6^8 \mod 9 \equiv 0 \to false \\
x = 7: &\quad 7^8 \mod 9 \equiv 4 \to false \\
x = 8: &\quad 8^8 \mod 9 \equiv 1 \to true
\end{aligned}
$$

   Hence, of the 7 numbers from $2 \to 8$, one of them gives an incorrect result and therefore the probability of returning true for this composite nunber is $1/7$.

3. What is the probability that `naiveIsPrime(9, 5)` returns true?

   Solution: By the same logic as above, the probability of picking a bad x is $1/7$ and the probability of doing this 5 times (picking no other number) is $(1/7)^5$. For perspective, this is roughly $1/17000 \approx 0.000059$.