UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab 5: Number Theory

Exercises from Lecture 10.

QUESTION 1

If possible (you need to check!), solve for x using the Chinese Remainder Theorem (CRT):

(a) $x \equiv 5 \pmod 7$ and $x \equiv 7 \pmod{10}$

(b) $x \equiv 3 \pmod 7$ and $x \equiv 7 \pmod{14}$

(c) $x \equiv 2 \pmod 6$ and $x \equiv 3 \pmod{11}$

Methodology: First find the GCD of p and q. If the GCD is equal to 1 (i.e. p and q are relatively prime) then a solution must exist; otherwise, there is no solution and CRT cannot be applied. If a solution exists, then use the CRT to find x.

More precisely, when $\gcd(p, q) = 1$, we apply CRT as follows. Let p, q be relatively prime. Let $n = pq$ be the modulus. Given integers c_1, c_2, there exists a unique integer x, $0 \leq x < n$, s.t.:

$$\begin{aligned} x &\equiv c_1 \pmod p \\ x &\equiv c_2 \pmod q \end{aligned}$$

Therefore, the CRT tells us that $x \equiv \frac{n}{p} y_1 c_1 + \frac{n}{q} y_2 c_2 \pmod n$ where:

$$\begin{aligned} y_1 &\equiv \left(\frac{n}{p}\right)^{-1} \pmod p \\ y_1 &\equiv q^{-1} \pmod p \\ qy_1 &\equiv 1 \pmod p \text{ [another way to write the above line]} \end{aligned}$$

and

$$\begin{aligned} y_2 &\equiv \left(\frac{n}{q}\right)^{-1} \pmod q \\ y_2 &\equiv p^{-1} \pmod q \\ py_2 &\equiv 1 \pmod q \text{ [another way to write the above line]} \end{aligned}$$

cont/...

We observe that y_1 is the inverse of q modulo p. Similarly, y_2 is the inverse of p modulo q.

See in Lecture 3, the slide entitled “Modular Inverses using the Euclidean Algorithm”. There exist 2 integers k_1, k_2 such that:

$$\begin{aligned} qy_1 + pk_1 &= 1 \\ py_2 + qk_2 &= 1 \end{aligned}$$

Observe that the unknowns are y_1, y_2, k_1, k_2. Then using back substitution, we find those values.

We replace y_1 and y_2 with the values that we have just found in:

$$\begin{aligned} x &\equiv \frac{n}{p} y_1 c_1 + \frac{n}{q} y_2 c_2 \pmod{n} \\ &\equiv qy_1 c_1 + py_2 c_2 \pmod{n} \end{aligned}$$

and we find x (do not forget to reduce modulo n!).

Example: Solve for x using the Chinese Remainder Theorem (CRT): $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 7$.

Let $p = 5$ and $q = 7$, and the modulus $n = pq = 35$. p and q are 2 prime numbers, so they are relatively prime, so a solution x must exist such that:

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Here, $c_1 = 2$ and $c_2 = 3$.

We now find y_1 and y_2 such that:

$$\begin{aligned} qy_1 &\equiv 1 \pmod p \\ 7y_1 &\equiv 1 \pmod 5 \end{aligned}$$

and

$$\begin{aligned} py_2 &\equiv 1 \pmod q \\ 5y_2 &\equiv 1 \pmod 7 \end{aligned}$$

cont/...

Let k_1, k_2 be 2 integers such that $7y_1 + 5k_1 = 1$ and $5y_2 + 7k_2 = 1$. We find that $y_1 = 3$ and $k_1 = -4$:

$$\begin{aligned}
7y_1 + 5k_1 &= 1 \\
y_1 &= \frac{1 - 5k_1}{7} \\
&= \frac{1 - 5 \times (-4)}{7} \\
&= \frac{1 + 20}{7} \\
&= \frac{21}{7} \\
&= 3
\end{aligned}$$

and that $y_2 = 3$ and $k_2 = -2$:

$$\begin{aligned}
5y_2 + 7k_2 &= 1 \\
y_2 &= \frac{1 - 7k_2}{5} \\
&= \frac{1 - 7 \times (-2)}{5} \\
&= \frac{1 + 14}{5} \\
&= \frac{15}{5} \\
&= 3
\end{aligned}$$

Now we use the values found for y_1 and y_2 in:

$$\begin{aligned}
x &\equiv \frac{n}{p} y_1 c_1 + \frac{n}{q} y_2 c_2 \pmod{n} \\
&\equiv q y_1 c_1 + p y_2 c_2 \pmod{n} \\
&\equiv (7 \times 3 \times 2) + (5 \times 3 \times 3) \pmod{35} \\
&\equiv 42 + 45 \pmod{35} \\
&\equiv 17 \pmod{35}
\end{aligned}$$

QUESTION 2

Find $\phi(20), \phi(21), \phi(22), \phi(23), \phi(24), \phi(25)$.

From the lecture slides:

- ϕ is the Euler function.
- $\phi(p) = p - 1$ where p is prime.

cont/...

- $\phi(pq) = (p-1)(q-1)$ where p, q are distinct primes.
- $n = p_1^{e_1} \cdots p_t^{e_t}$ where p_i are distinct primes, then:

$$\phi(n) = \prod_{i=1}^{t} p_i^{e_i - 1}(p_i - 1)$$

QUESTION 3

Find the discrete logarithm of the number 3 with regard to base 2 for:

(a) modulus $p = 5$

(b) modulus $p = 11$

(c) modulus $p = 29$

In other words, we need to find the value x such that $2^x = 3 \bmod p$ for the above values of p. To do so, we calculate $2^1 \bmod p$, $2^2 \bmod p$, $2^3 \bmod p$, $2^4 \bmod p$, etc. until finding x such that $2^x = 3 \bmod p$. More information can be found on slides 35 and 36 of Lecture 10.

QUESTION 4

Use the Fermat test to check whether the following numbers are prime or not:

- 979
- 983

Run the test **at most** 4 times with base values a equal to $2, 3, 11, 17$. In particular, we check whether $a^{979-1} \mod 979$ is equal to 1 or not, for $a = 2, 3, 11, 17$. Similarly, we check whether $a^{983-1} \mod 983$ is equal to 1 or not, for $a = 2, 3, 11, 17$. Check slides 13 and 14 of Lecture 10.

Note that these base values $a = 2, 3, 11, 17$ are not random, and in practice, fixed bases are usually applied.

Hint: $ab \mod n = (a \mod n)(b \mod n) \mod n$, and in particular, $(a^m)^k \mod n = (a^m \mod n)^k \mod n$.[1]

[1] See for instance `https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/fast-modular-exponentiation`.

QUESTION 5

We first recall the Miller-Rabin algorithm. Let n and u be odd, and v s.t. $n - 1 = 2^v u$:

(a) Pick a at random s.t. $1 < a < n - 1$

(b) Set $b = a^u \mod n$

(c) If $b = 1$ then return `probable prime`

(d) For $j = 0$ to $v - 1$:

- If $b = -1$ then return `probable prime`
- Else set $b = b^2 \mod n$

(e) Return `composite`

Use the Miller-Rabin algorithm for:

(a) $n = 17$.

We can easily see that n is prime. Let us see what the Miller-Rabin test tells us.

(b) $n = 15$.

We know that $15 = 3 \times 5$, hence n is **not** prime. Let us see what the Miller-Rabin test tells us.