CS 4823: Homework #5

Due on February 23, 2018

Christopher Tse

Problem 1

Let id be your student ID number. Solve the simultaneous congruences:

$$\begin{cases} x \equiv 2 \mod 297359071 \\ x \equiv 2 \mod 837582957839 \\ x \equiv 4 \mod id \end{cases}$$

Solution

Solving the simultaneous congruence using Chinese Remainder Theorem:

$m_1 = 297359071,\ m_2 = 837582957839,\ m_3 = id = 112971666$
$M = m_1 \cdot m_2 \cdot m_3 = 28137049647881671915457739954$
$M_1 = \frac{M}{m_1} = 94623142160279589774$
$M_2 = \frac{M}{m_2} = 33593149651082286$
$M_3 = \frac{M}{m_3} = 249062890228437207569$

Find integers y_i such that $y_i M_i \equiv 1 \mod m_i$. For each case, the Extended Euclidean Algorithm can be used. Using the `xgcd` function in Sage:

$y_1 M_1 \equiv 1 \mod m_1$
$94623142160279589774 y_1 \equiv 1 \mod 297359071$
$y_1 = 16501321$

$y_2 M_2 \equiv 1 \mod m_2$
$335931496510822864 y_2 \equiv 1 \mod 837582957839$
$y_2 = -358052305891$

$y_3 M_3 \equiv 1 \mod m_3$
$249062890228437207569 y_3 \equiv 1 \mod 112971666$
$y_3 = 42024317$

For the simultaneous congruence, x can be expressed as:

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i y_i M_i \\ &= (2 \cdot 16501321 \cdot 94623142160279589774) + (2 \cdot -358052305891 \cdot 33593149651082286) \\ &+ (4 \cdot 42024317 \cdot 249062890228437207569) \\ &= -2093339545472920502246967854 \end{aligned}$$

Problem 2

Part 1

Let id be your student ID number, p be the prime number 93935935937584760927320853927657, and q be the prime number 20395358947549853439147504976967820947509174847. Find an integer x such that $x^{37} \equiv id(\mod n)$, where $n = p \cdot q$.

Solution

$$\begin{aligned} x^{37} &\equiv id \mod n \\ x^{37} &\equiv 112971666 \mod n \\ x^{37} &\equiv \begin{cases} 112971666 \mod p \\ 112971666 \mod q \end{cases} \end{aligned}$$

We can reduce the exponents using Euler's Phi function then taking the modulus, but since p and q are so big, the resulting powers are still 37.

This gives us the result:

$$x = \begin{cases} 57156593804643713070162779699449 \\ 17296737745793791981935423565575416285014857800 \end{cases}$$

Part 2

If you do not know the factorization of n, can you find x quickly?

No

Problem 3

Find all the positive integers m such that $(\mathbb{Z}/m\mathbb{Z})^*$ has four elements.

Solution

Using Euler's Phi Function, we must find some integers m where $m = p^n$ such that p is prime and n is natural. $\phi(p^n) = p^n - p^{n-1}$. Therefore:

$$\begin{aligned} 4 &= p^n - p^{n-1} \\ 4 &= (p-1)p^{n-1} \end{aligned}$$

We can solve for p using the factorizations of 4. The factorizations of 4 are $1 \cdot 4$ and $2 \cdot 2$. Therefore:

$$\begin{aligned} p &= \begin{cases} 2 & \text{where } n = 3 \\ 5 & \text{where } n = 1 \end{cases} \\ &\Downarrow \\ m &= 2^3, 5^1 \\ m &= 5, 8 \end{aligned}$$

Using the factorization of 4 into $1 \cdot 4$ and $2 \cdot 2$ we can also use the multiplicative property of Euler's Phi function. Assume some x and y such that $m = xy$:

$$\phi(m) = \phi(x)\phi(y)$$

Using the factors 1 and 4:
$\phi(x) = 1,\ \phi(y) = 4$
$x = 2$

Using 5 from our answer above since $\phi(y) = \phi(m) = 4$, we get:
$\phi(m) = \phi(2)\phi(5)$
$m = 10$
(8 is ignored since $\phi(2)\phi(8) = \phi(16) \neq 4$)

However, the factors can be further split into $1 \cdot 2 \cdot 2$:

$\phi(x) = 1,\ \phi(y_1) = 2,\ \phi(y_2) = 2$
$x = 2,\ y_1 = 3,\ y_2 = 3$
$\phi(m) = \phi(2)\phi(3)\phi(6)$
$m = 12$

Putting them together, we get $m = 5, 8, 10, 12$

Problem 4

Calculate by hand $31^{30^{45}} \mod 35$ using Chinese Remainder Theorem

Solution First we split the modulus 35 into its prime factors 5 and 7:

$$\begin{cases} 31^{30^{45}} \mod 5 \\ 31^{30^{45}} \mod 7 \end{cases}$$

To reduce the exponent we take the modulus of the phi function of each factor:

$$\phi(5) = 4$$
$$\phi(7) = 6$$

We then obtain:

$$30^{45} \mod 4$$
$$30^{45} \mod 6$$

Since $30 \mod 6 = 0$ then $30^{45} \mod 6 = 0$ We can use fast modular exponentiation to calculate these:

$$30^{1+4+8+32} \mod 4 = (30 \cdot 30^4 \cdot 30^8 \cdot 30^{32}) \mod 4$$

$$30 \mod 4 = 2$$

$$30^4 \mod 4 = (30 \mod 4)(30 \mod 4)(30 \mod 4)(30 \mod 4) \mod 4$$
$$30^2 \mod 4 = (2 \cdot 2 \cdot 2 \cdot 2) \mod 4$$
$$30^2 \mod 4 = 16 \mod 4 = 0$$

We do not have to calculate the rest since we multiply the rest of the results. Since one is 0, the end result will be 0. This results in:

$$30^{45} \equiv 0 \mod 4$$
$$30^{45} \equiv 0 \mod 6$$

Replacing this into our original split simultaneous congruence, we get

Problem 4 continued on next page. . .

$$\begin{cases} x \equiv 31^{30^{45}} \equiv 31^0 \equiv 1 \mod 5 \\ x \equiv 31^{30^{45}} \equiv 31^0 \equiv 1 \mod 7 \end{cases}$$

We can now solve the resulting simultaneous congruence:

$$\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases}$$

$m_1 = 5, m_2 = 7$
$M = m_1 \cdot m_2 = 35$
$M_1 = \frac{M}{m_1} = 7$
$M_2 = \frac{M}{m_2} = 5$

Find integers y_i such that $y_i M_i \equiv 1 \mod m_i$:

$y_1 M_1 \equiv 1 \mod m_1$
$7y_1 \equiv 1 \mod 5$
$y_1 = -2$

$y_2 M_2 \equiv 1 \mod m_1$
$5y_2 \equiv 1 \mod 7$
$y_2 = 3$

For the simultaneous congruence, x can be expressed as:

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i y_i M_i \\ &= (1 \cdot -2 \cdot 7) + (1 \cdot 3 \cdot 5) \\ &= -14 + 15 \\ &= 1 \end{aligned}$$

Therefore, $31^{30^{45}} \mod 35 = 1$