CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 04A

1 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \; ; \; a \equiv 0 \pmod 5 \; ; \; a \equiv 0 \pmod 7, \tag{2}$$
$$b \equiv 0 \pmod 3 \; ; \; b \equiv 3 \pmod 5 \; ; \; b \equiv 0 \pmod 7, \tag{3}$$
$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 5 \; ; \; b \equiv 4 \pmod 7. \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

In the following parts, you will compute natural numbers a, b and c that satisfy the above 3 conditions and use them to find an x that indeed satisfies (1).

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).

Solution:

(a) Observe that $a+b+c \equiv 2+0+0 \pmod 3$, $a+b+c \equiv 0+3+0 \pmod 5$ and $a+b+c \equiv 0+0+4 \pmod 7$. Therefore $x = a+b+c$ indeed satisfies the conditions in (1).

(b) This question asks to find a number $0 \leq a < 3 \times 5 \times 7$ that is divisible by 5 and 7 and returns 2 when divided by 3. Let's first look at Part (b.i):

(b.i) Observe that $(5 \times 7) \equiv 35 \equiv 2 \pmod 3$. Multiplying both sides by 2, this means that $2 \times (5 \times 7) \equiv 4 \pmod 3 \equiv 1 \pmod 3$. So, the multiplicative inverse of 5×7, a^* is exactly 2. To verify this: observe that $(5 \times 7) \times 2 = 70 = 3 \times 23 + 1$. Therefore $(5 \times 7) \times 2 \equiv 1 \pmod 3$.

Consider $5 \times 7 \times a^*$. Since it is a multiple of 5 and 7, it is equal to 0 modulo either of these numbers. On the other hand, $5 \times 7 \times a^* \equiv 1 \pmod 3$, since a^* is precisely defined to be the multiplicative inverse of 5×7 modulo 3.

Consider $5 \times 7 \times (2 \times a^*) = 140$. It is a multiple of, and is therefore 0 modulo both 5 and 7. On the other hand, $5 \times 7 \times (2 \times a^*) \equiv 1 \times 2 \pmod 3$, for the same reason that a^* is defined to be the multiplicative inverse of 5×7 modulo 3.

Indeed observe that $5 \times 7 \times (2 \times a^*) = 140$ precisely satisfies the criteria required in Part (b). It is equivalent to 0 modulo 5 and 7 and $\equiv 2 \pmod 3$.

(c) Let's try to use a similar approach as Part (b). In particular, first observe that $3 \times 7 \equiv 21 \equiv 1 \pmod 5$. Therefore, b^*, the multiplicative inverse of 3×7 modulo 5 is in fact 1! So, let us consider $3 \times 7 \times (3 \times b^*) = 63$: this is a multiple of 3 and 7 and is therefore 0 modulo both these numbers. On the other hand, $3 \times 7 \times (3 \times b^*) \equiv 3 \pmod 5$ for the reason that b^* is the multiplicative inverse of 3×7 modulo 5.

(d) Yet again the approach of Part (b) proves to be useful! Observe that $3 \times 5 \equiv 15 \equiv 1 \pmod 7$. Therefore, c^*, the multiplicative inverse of 3×5 modulo 7 turns out to be 1. So, let us consider $3 \times 5 \times (4 \times c^*) = 60$: this is a multiple of 3 and 5. is therefore 0 modulo both these numbers. On the other hand, $3 \times 5 \times (4 \times c^*) \equiv 4 \pmod 7$ for the reason that c^* is the multiplicative inverse of 3×5 modulo 7.

(e) From Parts (b), (c) and (d) we find a choice of a, b, c (respectively $= 140, 63, 60$) which satisfues (2), (3) and (4). Together with Part (a) of the question, this implies that $x = a + b + c = 263$ satisfies the required criterion in (1).

To verify this: observe that,

$$263 = 87 \times 3 + 2,$$
$$263 = 52 \times 5 + 3,$$
$$263 = 37 \times 7 + 4.$$

2 CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations $\mod 385$). Solve the system using the Chinese Remainder Theorem. What is $3^{302} \mod 385$?

Solution:

(a) $385 = 11 \times 7 \times 5$.

(b) Since $3^4 \equiv 1 \pmod 5$, $3^{302} \equiv 3^{4(75)} \cdot 3^2 \equiv 4 \pmod 5$.
Since $3^6 \equiv 1 \pmod 7$, $3^{302} \equiv 3^{6(50)} \cdot 3^2 \equiv 2 \pmod 7$.
Since $3^{10} \equiv 1 \pmod{11}$, $3^{302} \equiv 3^{10(30)} \cdot 3^2 \equiv 9 \pmod{11}$.

(c) $x \equiv 4 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 9 \pmod{11}$.
The answer we get using CRT is $x \equiv 9 \pmod{385}$. So $3^{302} \equiv 9 \pmod{385}$.

3 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod m$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod m$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod m$, where $i > j$, what can you say about $a^{i-j} \pmod m$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod m$. What is k in terms of i and j?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.
The Pigeonhole principle applies here - we have m boxes that represent the different unique values that a^k can take on $\pmod m$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the m boxes. As soon as we have more than m objects (in other words, we reach a^{m+1} in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod m$.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion.

If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod m,\\
a^{i-j} &\equiv 1 && \pmod m.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod m$ as $a^{i-j-1}a \equiv 1 \pmod m$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod m$.