Written Assignment 8

CS 135-B/LF

April 13, 2024

1

Using the division algorithm, we can gather that all integers can be represented by some multiple of 6 plus some integer $0 \leq q \leq 5$. We can denote this as $6k + q$. If q is equal to 0, 2, or 4, the sum $6k + q$ will be even, and therefore it cannot represent the primes p or $p + 2$. If q is equal to 3 then $6k + q$ will be divisible by 3 and again, cannot represent p or $p + 2$. This leaves only the options $q = 1$ and $q = 5$. Again using the division algorithm we understand that the case where q = 5, $6k + 5$, can be written as $6k - 1$. As such, for any prime $p = 6k - 1$, we can also represent the prime $p + 2$ as $6k + 1$. ■

2

2.a

To find the inverse of 20 mod 1343, we need to find $20x \equiv 1(\mod 1343)$:

Line	Q	R	x	y
1		20	1	0
2		1343	0	1
3	0	20	1	0
4	67	3	-67	1
5	6	2	403	-6
6	1	1	-470	7
7	2	0	1343	-20

Using line 6, we know that $-470 \cdot 20 + 7 \cdot 1343$ and as such the multiplicative inverse for 20 mod 1343 is -470. If we need it to be positive, we can add 1343 to -470 and retrieve 873 because $-470 \equiv 873(\mod 1343)$.

2.b

Using multiplicative inverse 20 mod 1343 we can gather that one possible $x = 7 \cdot 873 = 6111$ so $20 \cdot 6111 \equiv 122220 \equiv 7(\mod 1343)$. Generally, $x \equiv 122220(\mod 1343)$.

3

3.a

Find $\phi(100)$.
We can find that $100 = 2^2 \times 5^2$. Therefore 100 has prime divisors 2 and 5.
Fact from Lecture 20: For prime divisors of n $p_1, p_2, \ldots, p_k$, $\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$
This gives us $\phi(100) = 100(1 - 1/2)(1 - 1/5)$ which works out to 40.

3.b

We can use mod 100 to find the last two digits of any number. Thus we now must solve $17^{800,000,000,000,000,000,000,000,000,000,000,000,001} \mod 100$.
To make sure we can use Euler's Theorem, we can check that gcd(17,100) = 1. Since 17 is prime this statement is clearly true.
We know by 3.a that $\phi(100) = 40$, and using Euler's theorem we can deduce that $17^{\phi(100)} \equiv 17^{40} \equiv 1(\mod 100)$. We can break $17^{800,000,000,000,000,000,000,000,000,000,000,000,001}$ into $17^1 \cdot 17^{8\cdot 10^{35}}$, then $17^1 \cdot 17^{80\cdot 10^{34}}$, then $17^1 \cdot 17^{40^{2\cdot 10^{34}}}$. Then we can deduce that $17 * (17^{40})^{10^{34}} \equiv 17 * 1^{10^{34}} \equiv 17(\mod 100)$. This can be rewritten as $17^{800,000,000,000,000,000,000,000,000,000,000,000,001} \equiv 17(\mod 100)$. Therefore, the last two digits of $17^{800,000,000,000,000,000,000,000,000,000,000,000,001}$ are 17.

4

We are given the following:

$$\begin{aligned} x &\equiv 8 \mod 11 \\ x &\equiv 5 \mod 17 \\ x &\equiv 16 \mod 29 \\ x &\equiv 24 \mod 31 \end{aligned}$$

Along with the information that x has no more than 5 digits. Since none of 11, 17, 29, and 31 have any common factors, the computer scientist son might have realized that this is a setup for the Chinese Remainder Theorem. We'll start by gathering:

$$\begin{aligned} m &= 11 \cdot 17 \cdot 29 \cdot 31 = 168113 \\ M_1 &= \phantom{11 \cdot{}} 17 \cdot 29 \cdot 31 = 15283 \\ M_2 &= 11 \cdot \phantom{17 \cdot{}} 29 \cdot 31 = 9889 \\ M_3 &= 11 \cdot 17 \cdot \phantom{29 \cdot{}} 31 = 5797 \\ M_4 &= 11 \cdot 17 \cdot 29 \phantom{{}\cdot 31} = 5423 \end{aligned}$$

Now we need to find the multiplicative inverses of

$$\begin{aligned} M_1 &\equiv 15283(\mod 11) \\ M_2 &\equiv 9889(\mod 17) \\ M_3 &\equiv 5797(\mod 29) \\ M_4 &\equiv 5423(\mod 31). \end{aligned}$$

For each M_k we'll call its multiplicative inverse y_k. Using the Euclidean algorithm, we can calculate that

$$\begin{aligned} y_1 &= 3 \\ y_2 &= 10 \\ y_3 &= 19 \\ y_4 &= 15 \end{aligned}$$

Now we can find our solution by calculating

$$\begin{aligned} &8 \cdot 15283 \cdot 3 \\ &+ 5 \cdot 9889 \cdot 10 \\ &+ 16 \cdot 5797 \cdot 19 \\ &+ 24 \cdot 5423 \cdot 15 \\ &= 4575810 \end{aligned}$$

and taking 4575810 mod 168113 which is equal to 36759. With a quick calculation we can find that 36759 matches all of the requirements to be congruent to x in all given cases. Since this number also has 5 digits, it must be the vault combination.

5

We are given positive integers a, b and an integer c where $a \mid c$, $b \mid c$ and $\gcd(a, b) = 1$.
According to Bezout's theorem, for positive integers a and b, there are integers x and y where

$$\gcd(a, b) = xa + yb$$

Since $b \mid c$, it follows that $ab \mid ac$ and $ac \mid xac$. Since $a \mid c$, it follows that $ab \mid cb$ and $cb \mid ycb$. By the division algorithm, $ab \mid xac$ and $ab \mid ycb$. We can sum these multiples of ab and still have a multiple of ab, therefore $ab \mid (xac + ycb) = c(xa + yb)$. By Bezout's theorem, $xa + yb = \gcd(a, b) = 1$ which is given. Now we know that $ab \mid xac + ycb \implies ab \mid c(1) \implies ab \mid c$ which was to be proven. ■

6

Let's take $a = 2$, $b = 2$, and $c = 2$. $\gcd(2, 2) = 2 > 1$, $2 \mid 2 \implies a \mid c$ and $b \mid c$, therefore the premises are true. However, $ab = 2 \times 2 = 4$ and $4 \nmid 2 \implies ab \nmid c$. ■