Mathematics 546 Homework.

We have seen that if a, n, x, y, b are integers and

$$ax + ny = b$$

then is we reduce modulo n and use that $ny \equiv 0 \pmod{n}$ we get that

$$ax \equiv b \pmod{n}.$$

Conversely if

$$ax \equiv b \pmod{n}$$

then $n \mid (ax - b)$ which means there is an integer k with $ax - b = kn$. This can be rewritten as

$$ax + (-k)n = b$$

and this if we set $y = -k$ this is

$$ax + by = b.$$

Therefore solving

$$ax \equiv b \pmod{n}$$

for x is the same as solving

$$ax + ny = b$$

for x and y and then just using the x value.

We are experts as using the Euclidean algorithm to finding a solution to

$$ax + ny = \gcd(a, n).$$

In particular when $\gcd(a, n) = 1$ we can find x and y with

$$ax + ny = 1.$$

Reducing modulo n lets us find a solution to $ax \equiv 1 \pmod{n}$.

Definition 1. It $n \geq 1$ and a are integers with $\gcd(a, n) = 1$ then any solution to

$$ax \equiv 1 \pmod{n}$$

is an ***inverse of*** a ***modulo*** n. We will denote such an inverse by $\widehat{a}$. □

To be explicit $\widehat{a}$ is an integer such that

$$\widehat{a}a \equiv 1 \pmod{n}.$$

Theorem 2. *Let a, b, n be integers with $n \geq 1$ and $\gcd(a, n) = 1$. Then the congruence*

$$ax \equiv b \pmod{n}$$

has a solution. It is given by

$$x \equiv \widehat{a}b.$$

Proof. We just check directly that $x \equiv \widehat{a}b \pmod{n}$ works:

$$\begin{aligned} ax &\equiv a(\widehat{a}b) \pmod{n} \\ &\equiv (a\widehat{a})b \pmod{n} \\ &\equiv 1b \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

□

The solution given in Theorem 2 is unique modulo n as we now show. The proof is based on the following, which we have used several times before (but here we change the notation a bit to match what we are currently working on).

Theorem 3. *Let a, x, n be integers with $n \geq 1$ and $\gcd(a, n) = 1$. Then $n \mid ax$ implies $n \mid x$.* □

Here is the uniqueness result:

Theorem 4. *If a, n, b are integers with $n \geq 1$ and $\gcd(a, n) = 1$, and x_1 and x_2 satisfy*

$$\begin{aligned} ax_1 &\equiv b \pmod{n} \\ ax_2 &\equiv b \pmod{n} \end{aligned}$$

then

$$x_1 \equiv x_2 \pmod{n}.$$

Problem 1. Prove this. *Hint:* Note

$$\begin{aligned} ax_2 - ax_1 &\equiv b - b \pmod{n} \\ &0 \pmod{n}. \end{aligned}$$

Use this to show $n \mid a(x_2 - x_1) = ax$ where $x = x_2 - x_1$ and then use Theorem 3. □

As an example let us solve

$$17x \equiv 42 \pmod{132}.$$

To start we saw in the Lesson
`http://ralphhoward.github.io/Classes/Fall2020/546/Lesson_2/`
that

$$x \equiv 101 \pmod{132}.$$

is a solution to

$$17x \equiv 1 \pmod{132}.$$

therefore we have that

$$\widehat{17} \equiv 101 \pmod{132}$$

is the inverse of 17 modulo 132. Whence the solution to $17x \equiv 42 \pmod{132}$ is

$$x \equiv \widehat{17} \cdot 42 \equiv 101 \cdot 42 \equiv 4242 \pmod{132}.$$

To get a nicer looking answer use that if 132 is divided into 4242 the remainder is 18 and therefore

$$x \equiv 18 \pmod{132}$$

is a pleasanter looking solution. (And you can check that $17(18) = 306 = 2(132) + (42)$ which implies $17 \cdot 18 \equiv 42 \pmod{132}$.)

Problem 2. Solve the following
(a) $14x \equiv 8 \pmod{51}$
(b) $3x \equiv 59 \pmod{538}$

Now that we know how to solve $ax \equiv b \pmod{n}$ when $\gcd(a, n) = 1$, it is natural to ask what happens when $\gcd(a, n) > 1$. We now work this out (you should compare this with pages 30–33 in the text). As we saw above

$$ax \equiv b \pmod{n}$$

has a solution for x if and only if

$$ax + ny = b$$

has a solution (x, y) with x and y integers.

Proposition 5. *If*

$$ax \equiv b \pmod{n}$$

has a solution, then

$$\gcd(a, n) \mid b.$$

(That is if the congruence has a solution, then $\gcd(a, b)$ *divides* b*.)*

Problem 3. Prove this. *Hint:* If the congruence has a solution, then there are integers x and y with

$$ax + yn = b.$$

Set $d = \gcd(a, n)$. Then d is a divisor of both of a and n therefore there are integers a_1 and n_1 such that $a = a_1 d$ and $n = n_1 d$. Use this in $ax + yn = b$ to show $d \mid b$. $\square$

Proposition 6. *If* a *and* b *are integers, not both zero, and* $d = \gcd(a, b)$*. Then the integers*

$$a_1 = \frac{a}{d} \qquad b_1 = \frac{b}{d}$$

are relatively prime. (That is $\gcd(a_1, b_1) = 1$*.)*

Problem 4. Prove this. *Hint:* By the GCD is a Linear Combination Theorem we have that there are integers x and y with

$$ax + by = d.$$

And we also have $a = a_1 d$ and $b = b_1 d$. Put these facts together to get that

$$a_1 x + b_1 y = 1$$

which implies $\gcd(a_1, b_1) = 1$. $\square$

Proposition 7. *If a, n, b are integers with $n \geq 1$ and so that $\gcd(a, n) \mid b$, then*

$$ax \equiv b \pmod{n}$$

has solutions. These are found by solving

$$a_1 x \equiv b_1 \pmod{n_1}$$

where

$$a_1 = \frac{a}{\gcd(a,n)}, \qquad b_1 = \frac{b}{\gcd(a,n)}, \quad n_1 = \frac{n}{\gcd(a,n)}.$$

Problem 5. Prove this. *Hint:* First a bit of notation. Let $d = \gcd(a, n)$. Then form the definitions of a_1, b_1, and n_1 we have

$$a = a_1 d, \quad b = b_1 d, \quad n = n_1 d.$$

We know that $ax \equiv b \pmod{n}$ has solution if and only if there are integers x and y with

$$ax + ny = b.$$

But this can be rewritten as

$$a_1 dx + n_1 dy = b_1 d.$$

Dividing out the d gives that this is equivalent to solving

$$a_1 x + n_1 y = b_1$$

which in turn has a solution if and only if

$$a_1 x \equiv b_1 \pmod{n_1}.$$

Now use Proposition 6 to see that $\gcd(a_1, n_1) = 1$ and explain why this implies $a_1 x \equiv b_1 \pmod{n_1}$ has solutions. □

Problem 6. In the following congruences either solve them or explain why they have no solutions.

(a) $15x \equiv 33 \pmod{65}$.
(b) $15x \equiv 32 \pmod{65}$.
(c) $38x \equiv 52 \pmod{101}$. □

Given a positive integer n and $a \in \mathbb{Z}$ we have defined the ***congruence class*** of a modulo n as

$$[a]_n = \{x : x \equiv a \pmod{n}\}$$

and shown

$$[a]_n = [b]_n \qquad \Longleftrightarrow \qquad a \equiv b \pmod{n}.$$

For each n there are exactly n congruence classes modulo n and they are

$$[0]_n,\ [1]_n,\ \cdots,\ [n-1]_n.$$

This is because two numbers are congruence modulo n if and only if they have the same remainder when divided by n and the possible remainders when dividing by n are $0, 1, 2, \ldots, (n-1)$. Let $\mathbb{Z}_n$ be the set of all congruence classes modulo n. That is

$$\begin{aligned}
\mathbb{Z}_2 &= \{[0]_2, [1]_2\} \\
\mathbb{Z}_3 &= \{[0]_3, [1]_3, [2]_3\} \\
\mathbb{Z}_4 &= \{[0]_4, [1]_4, [2]_4, [3]_4\} \\
\mathbb{Z}_5 &= \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\} \\
\mathbb{Z}_6 &= \{[0]_6, [1]_6, [2]_6, [3]_6, [5]_6, [4]_6\}
\end{aligned}$$

and in general

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$$

We have defined addition and multiplication of the congruence classes by

$$[a]_n + [b]_n = [a+b]_n, \qquad [a]_n[b]_n = [ab]_n.$$

At the end of the document there is a list of the addition and multiplication for $\mathbb{Z}_n$ for $2 \leq n \leq 12$.

Recall that $[a]_n \in \mathbb{Z}_n$ is a ***unit*** (or is ***invertible***) if and only if there is $[b]_n \in \mathbb{Z}_n$ with $[a]_n[b]_n = 1$. In this case we call $[b]_n$ and write $[b]_n^{-1}$.

For example, using the table below, we have that the units in $\mathbb{Z}_{12}$ are $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$ and

$$[1]_{12}^{-1} = [1]_{12}, \quad [5]_{12}^{-1} = [5]_{12}, \quad [7]_{12}^{-1} = [7]_{12}, \quad [11]_{12}^{-1} = [11]_{12}$$

Or in $\mathbb{Z}_5$ the units are $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$ and their inverses are

$$[1]_5^{-1} = [1]_5^{-1}, \quad [2]_5^{-1} = [3]_5, \quad [3]_5^{-1} = [2]_5, \quad [4]_5^{-1} = [4]_5.$$

Problem 7. What are the units in $\mathbb{Z}_{12}$? What are their inverses? □

Problem 8. What are the units in $\mathbb{Z}_7$? What are their inverses? □

Proposition 8. *The element* $[a]_n \in \mathbb{Z}_n$ *is a unit if and only if* $\gcd(a, n) = 1$.

Problem 9. Prove this. □

Problem 10. Find the inverse of $[13]_{57}$ in $\mathbb{Z}_{57}$. □

We have also defined the ***Euler*** ϕ ***function*** as

$$\phi(n) = \text{the number of units in } \mathbb{Z}_n.$$

Problem 11. Compute $\phi(n)$ for $2 \leq n \leq 12$. □

Problem 12. Let p be a prime number.

(a) Let $[a]_p \in \mathbb{Z}_p$ with $[a]_p \neq [0]_p$. Show that $[a]_p$ is a unit. *Hint:* As $[a]_p \neq [0]_p$ we have that p is not a factor of a. Use this and that p is prime to show $\gcd(a, p) = 1$ and therefore that $ax \equiv 1 \pmod{n}$ has a solution.

(b) Show $\phi(p) = p - 1$. □

Appendix: Addition and multiplication tables for $\mathbb{Z}_n$

Here are the addition and multiplication for small values of n. In writing these I use the simplified notation $[a]$ rather than $[a]_n$.

$\mathbb{Z}_2$:

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

×	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

$\mathbb{Z}_3$:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\mathbb{Z}_4$:

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\mathbb{Z}_5$:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

$\mathbb{Z}_6$:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_7$:

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_8$:

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_9$:

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[8]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_{10}$:

$+$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]

$\times$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[2]	[0]	[2]	[4]	[6]	[8]	[0]	[2]	[4]	[6]	[8]
[3]	[0]	[3]	[6]	[9]	[2]	[5]	[8]	[1]	[4]	[7]
[4]	[0]	[4]	[8]	[2]	[6]	[0]	[4]	[8]	[2]	[6]
[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]
[6]	[0]	[6]	[2]	[8]	[4]	[0]	[6]	[2]	[8]	[4]
[7]	[0]	[7]	[4]	[1]	[8]	[5]	[2]	[9]	[6]	[3]
[8]	[0]	[8]	[6]	[4]	[2]	[0]	[8]	[6]	[4]	[2]
[9]	[0]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_{11}$:

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[10]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]	[0]	[4]	[8]	[1]	[5]	[9]	[2]	[6]	[10]	[3]	[7]
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]
[6]	[0]	[6]	[1]	[7]	[2]	[8]	[3]	[9]	[4]	[10]	[5]
[7]	[0]	[7]	[3]	[10]	[6]	[2]	[9]	[5]	[1]	[8]	[4]
[8]	[0]	[8]	[5]	[2]	[10]	[7]	[4]	[1]	[9]	[6]	[3]
[9]	[0]	[9]	[7]	[5]	[3]	[1]	[10]	[8]	[6]	[4]	[2]
[10]	[0]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_{12}$:

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[10]	[11]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[10]	[11]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[10]	[11]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[10]	[11]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[10]	[10]	[11]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[11]	[11]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[0]	[2]	[4]	[6]	[8]	[10]
[3]	[0]	[3]	[6]	[9]	[0]	[3]	[6]	[9]	[0]	[3]	[6]	[9]
[4]	[0]	[4]	[8]	[0]	[4]	[8]	[0]	[4]	[8]	[0]	[4]	[8]
[5]	[0]	[5]	[10]	[3]	[8]	[1]	[6]	[11]	[4]	[9]	[2]	[7]
[6]	[0]	[6]	[0]	[6]	[0]	[6]	[0]	[6]	[0]	[6]	[0]	[6]
[7]	[0]	[7]	[2]	[9]	[4]	[11]	[6]	[1]	[8]	[3]	[10]	[5]
[8]	[0]	[8]	[4]	[0]	[8]	[4]	[0]	[8]	[4]	[0]	[8]	[4]
[9]	[0]	[9]	[6]	[3]	[0]	[9]	[6]	[3]	[0]	[9]	[6]	[3]
[10]	[0]	[10]	[8]	[6]	[4]	[2]	[0]	[10]	[8]	[6]	[4]	[2]
[11]	[0]	[11]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]