الجامعة اللبنانية
كلية الإعلام والتوثيق

Chapter 3

Lecture : Exercises & Correction

Prepared by:

- Dr. Abbas Rammal
- Dr. Rabih Assaf

Ex 1.

Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a \pmod{13}$.
b) $c \equiv 11b \pmod{13}$.
c) $c \equiv a + b \pmod{13}$.
d) $c \equiv 2a + 3b \pmod{13}$.
e) $c \equiv a^2 + b^2 \pmod{13}$.
f) $c \equiv a^3 - b^3 \pmod{13}$.

Solution Exercise 1

DEFINITIONS

Division algorithm Let a be an integer and d a positive integer. Then there are unique integers q and r with $0 \leq r < d$ such that $a = dq + r$
q is called the **quotient** and r is called the **remainder**

$$q = a \textbf{ div } d$$

$$r = a \textbf{ mod } d$$

Theorem 5 Let m be a positive integer. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$, then $a + c \equiv b + d (\text{mod } m)$ and $ac \equiv bd (\text{mod } m)$.

SOLUTION

$$a = 4 \textbf{ (mod } 13)$$

$$b \equiv 9 \textbf{ (mod } 13)$$

$$0 \leq c \leq 12$$

(a) Use theorem 5:

$$c \equiv 9a \textbf{ (mod } 13)$$

$$= 9 \cdot 4 \textbf{ (mod } 13)$$

$$= 36 \textbf{ (mod } 13)$$

$$= 10 \textbf{ (mod } 13)$$

We then obtain $c = 10$ with $0 \leq c \leq 12$.

(b) Use theorem 5:

$$\begin{aligned} c &\equiv 11b \,(\mathbf{mod}\ 13) \\ &= 11 \cdot 9 \,(\mathbf{mod}\ 13) \\ &= 99 \,(\mathbf{mod}\ 13) \\ &= 8 \,(\mathbf{mod}\ 13) \end{aligned}$$

We then obtain $c = 8$ with $0 \leq c \leq 12$.

(c) Use theorem 5:

$$\begin{aligned} c &\equiv a + b \,(\mathbf{mod}\ 13) \\ &= 4 + 9 \,(\mathbf{mod}\ 13) \\ &= 13 \,(\mathbf{mod}\ 13) \\ &= 0 \,(\mathbf{mod}\ 13) \end{aligned}$$

We then obtain $c = 0$ with $0 \leq c \leq 12$.

(d) Use theorem 5:

$$\begin{aligned} c &\equiv 2a + 3b (\mathbf{mod}\ 13) \\ &= 2 \cdot 4 + 3 \cdot 9 \,(\mathbf{mod}\ 13) \\ &= 8 + 27 \,(\mathbf{mod}\ 13) \\ &= 35 \,(\mathbf{mod}\ 13) \\ &= 9 \,(\mathbf{mod}\ 13) \end{aligned}$$

We then obtain $c = 9$ with $0 \leq c \leq 12$.

(e) Use theorem 5:

$$\begin{aligned} c &\equiv a^2 + b^2 \,(\mathbf{mod}\ 13) \\ &= 4^2 + 9^2 \,(\mathbf{mod}\ 13) \\ &= 16 + 81 \,(\mathbf{mod}\ 13) \\ &= 97 \,(\mathbf{mod}\ 13) \\ &= 6 \,(\mathbf{mod}\ 13) \end{aligned}$$

We then obtain $c = 6$ with $0 \leq c \leq 12$.

(f) Use theorem 5:

$$\begin{aligned} c &\equiv a^3 - b^3 \,(\mathbf{mod}\ 13) \\ &= 4^3 - 9^3 \,(\mathbf{mod}\ 13) \\ &= 64 - 729 \,(\mathbf{mod}\ 13) \\ &= -665 \,(\mathbf{mod}\ 13) \\ &= -2 \,(\mathbf{mod}\ 13) \\ &= 11 \,(\mathbf{mod}\ 13) \end{aligned}$$

We then obtain $c = 11$ with $0 \leq c \leq 12$.

Ex 2.

Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \bmod m = b \bmod m$.

EX 3.

Let m be a positive integer. Show that $a \bmod m = b \bmod m$ if $a \equiv b \pmod{m}$.

EX 4.

Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with $m \geq 2$, then $a - c \equiv b - d \pmod{m}$.

Solution Exercise 2

SOLUTION

Given: m is a positive integer and a **mod** $m = b$ **mod** m

To proof: $a \equiv b \pmod{m}$

PROOF

a **mod** $m = b$ **mod** m indicates that there exist an integer q_1 such that:

$$a \textbf{ mod } m = mq_1 + b$$

b **mod** $m = a$ **mod** m indicates that there exist an integer q_2 such that:

$$b \textbf{ mod } m = mq_2 + a$$

Since a **mod** $m = b$ **mod** m:

$$mq_2 + a = mq_1 + b$$

Subtract b from each side of the equation:

$$mq_2 + a - b = mq_1$$

Subtract mq_2 from each side of the equation:

$$a - b = mq_1 - mq_2$$

Factorize the right side of the equation:

$$a - b = m(q_1 - q_2)$$

Since q_1 and q_2 are both integers, their difference $q_1 - q_2$ is also an integer.

By the definition of **divides**, we have then shown that m divides $a - b$. By the definition of equivalent modulo m:

$$a \equiv b \pmod{m}$$

□

Solution Exercise 3

Assume it is not the case $a \pmod m = b \pmod m$. Then, $a \pmod m \neq b \pmod m$. This means that $\frac{a}{m}$ and $\frac{b}{m}$ do not have the same remainders, and they dont have the same quotients. Then, $a = mq_1 + r_1$ and $b = mq_2 + r_2$, where, q_1 and $q_2 \, \epsilon Z$, and, $0 \leq r_1 < m$ and $0 \leq r_2 < m$.

$$\begin{aligned} a - b &= mq_1 + r_1 - mq_2 - r_2 \\ &= m(q_1 - q_2) + r_1 - r_2 \end{aligned}$$

By definition, $m \nmid (a-b)$. Since $m \mid (a-b)$ is equivalent to $a \equiv b \pmod m$, $a \not\equiv b \pmod m$.
It has been shown that if $a \pmod m \neq b \pmod m$, then $a \not\equiv b \pmod m$.
Thus by contraposition, if $a \equiv b \pmod m$, then $a \pmod m = b \pmod m$.
$Q.E.D$

Solution Exercise 4

SOLUTION

Given: a, b, c, d, m are integers with $m \geq 2$

$$a \equiv b \pmod{m}$$
$$c \equiv d \pmod{m}$$

To proof: $a - c \equiv b - d \pmod{m}$

PROOF

Using the definition of congruent on $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$:

$$m \text{ divides } a - b$$
$$m \text{ divides } c - d$$

By the definition of "divides", there then exist integers f and g such that:

$$a - b = mf$$
$$c - d = mg$$

Let us subtract the previous two equations:

$$a - b - (c - d) = mf - mg$$

Use distributive property:

$$a - b - c + d = m(f - g)$$

Regroup the variables:

$$(a - c) - (b - d) = m(f - g)$$

By the definition of divides, we then obtained that m divides $(a-c)-(b-d)$.

By the definition of congruent, we have then shown that $a-c \equiv b-d \pmod{m}$

□

EX 5.

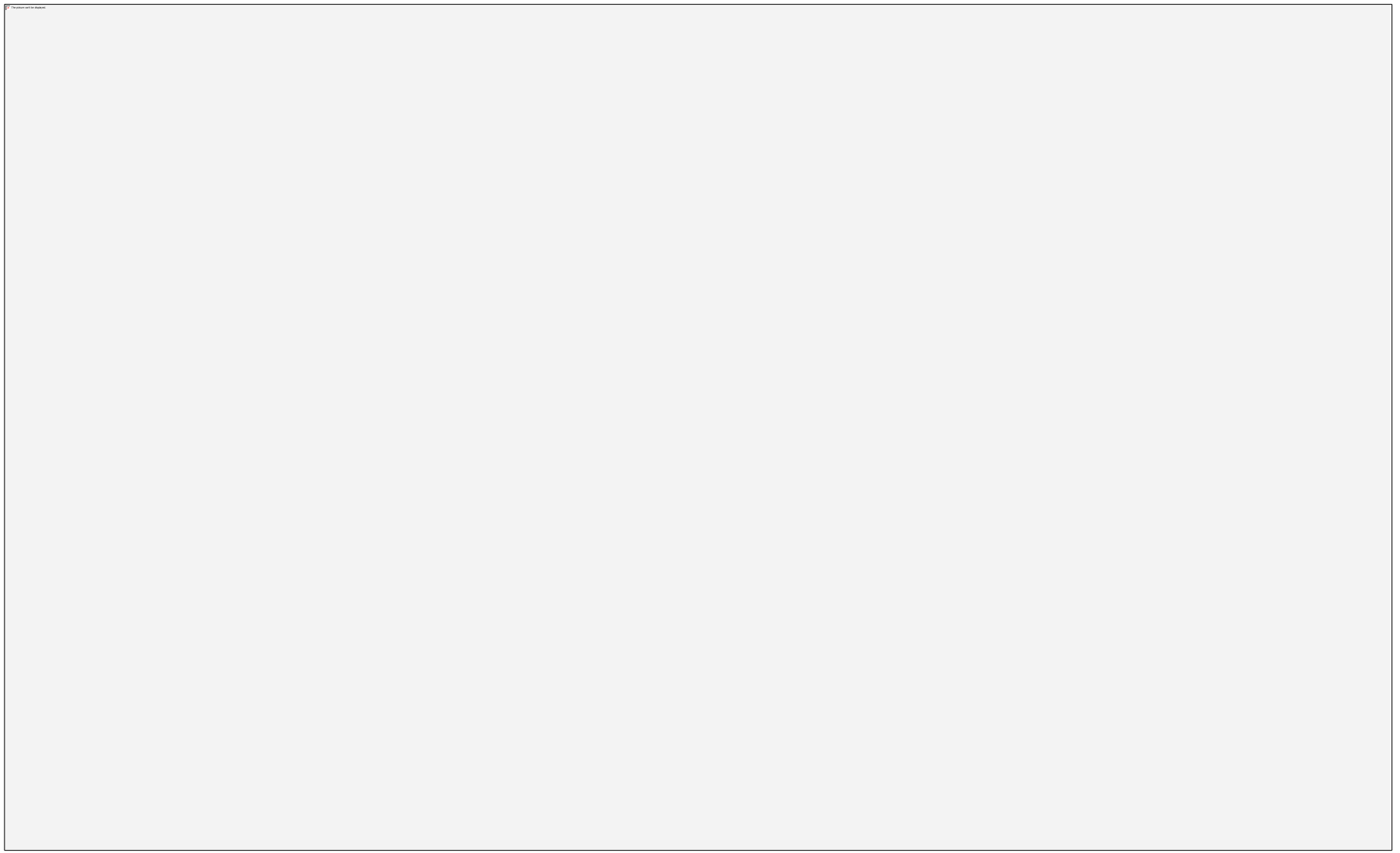
Show that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

EX 6.

Show that if a, b, c, and m are integers such that $m \geq 2$, $c > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

Solution Exercise 5

Solution Exercise 6



EX 7.

Find the integer a such that

a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$.

b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$.

c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$.

EX 8.

Convert the decimal expansion of each of these integers to a binary expansion.

a) 231 **b)** 4532 **c)** 97644

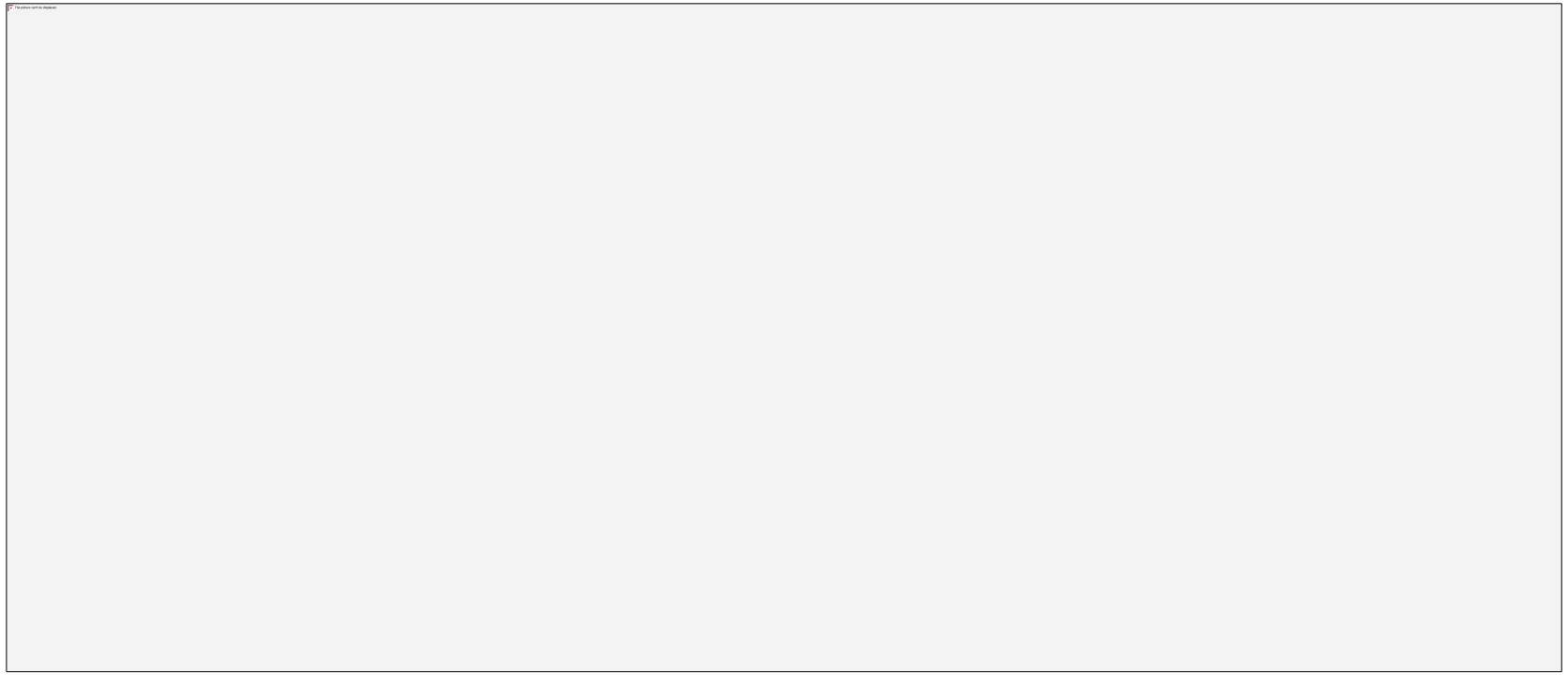
EX 9.

Convert the binary expansion of each of these integers to a decimal expansion.

a) $(1\ 1111)_2$ **b)** $(10\ 0000\ 0001)_2$

c) $(1\ 0101\ 0101)_2$ **d)** $(110\ 1001\ 0001\ 0000)_2$

Solution Exercise 7



(c)

$$a \equiv 99 \pmod{41}$$

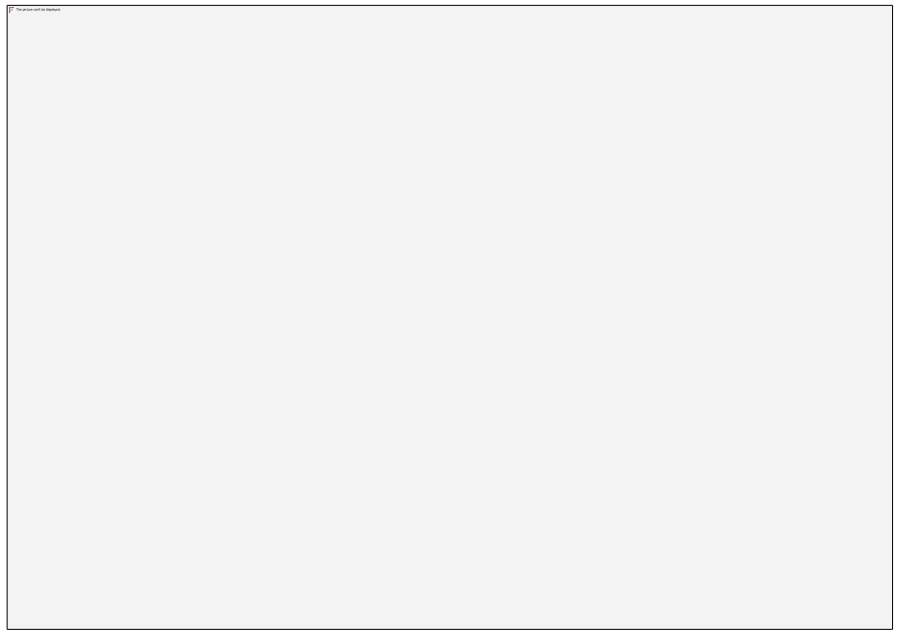
We can find a such that $100 \leq a \leq 140$ by consecutively adding 41 to 99 until we obtain a value between 100 and 140.

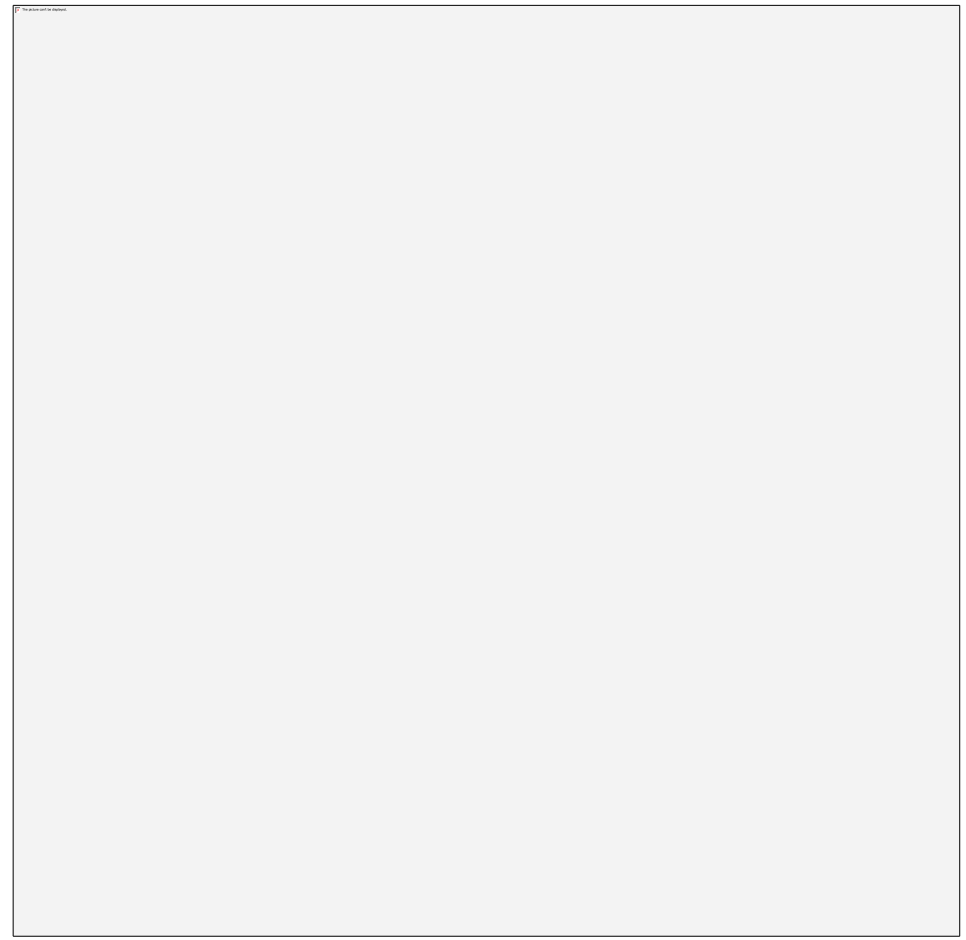
$$\begin{aligned} a &\equiv 99 \pmod{41} \\ &\equiv 99 + 41 \pmod{41} \\ &\equiv 140 \pmod{41} \end{aligned}$$

Since 140 is between 100 and 140 (including):

$$a = 140$$

Solution Exercise 8


The picture can't be displayed.


The picture can't be displayed.

c)

$$
\begin{aligned}
97644 &= 2 \cdot 48822 + 0 \\
48822 &= 2 \cdot 24411 + 0 \\
24411 &= 2 \cdot 12205 + 1 \\
12205 &= 2 \cdot 6102 + 1 \\
6102 &= 2 \cdot 3051 + 0 \\
3051 &= 2 \cdot 1525 + 1 \\
1525 &= 2 \cdot 762 + 1 \\
762 &= 2 \cdot 381 + 0 \\
381 &= 2 \cdot 190 + 1 \\
190 &= 2 \cdot 95 + 0 \\
95 &= 2 \cdot 47 + 1 \\
47 &= 2 \cdot 23 + 1 \\
23 &= 2 \cdot 11 + 1 \\
11 &= 2 \cdot 5 + 1 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0 \\
1 &= 2 \cdot 0 + 1 \\
\Rightarrow (97644)_{10} &= (10111110101101100)_2
\end{aligned}
$$