

MATH 8: ASSIGNMENT 25

APRIL 19, 2026

SUMMARY OF PREVIOUS

Recall that we say that t is inverse of $a \pmod n$ if $at \equiv 1 \pmod n$.

Theorem. *A number a has an inverse mod n if and only if a is relatively prime with n , i.e. $\gcd(a, n) = 1$.*

If a has an inverse mod n , then we can easily solve equations of the form

$$ax \equiv b \pmod n$$

Namely, just multiply both sides by inverse of a .

LEAST COMMON MULTIPLE

Theorem. *Let a, b be relatively prime. Then any common multiple of a, b is a multiple of ab ; in particular, the least common multiple of a, b is ab .*

Proof. Assume that m is a common multiple of a, b . Then $m = ta$ for some t . Since m is also a multiple of b , we get $ta \equiv 0 \pmod b$. Since a, b are relatively prime, a is invertible mod b . Multiplying both sides of congruence by inverse of $a \pmod b$, we get $t \equiv 0 \pmod b$, so t is divisible by b , i.e. $t = sb$ for some t . Thus, $m = ta = sab$ is a multiple of ab . \square

CHINESE REMAINDER THEOREM

The previous result can be stated as follows: if a, b are relatively prime, then

$$\begin{aligned}x &\equiv 0 \pmod a \\x &\equiv 0 \pmod b\end{aligned}$$

happens if and only if $x \equiv 0 \pmod{ab}$.

This is a special case of the following famous result.

Theorem (Chinese Remainder Theorem). *Let a, b be relatively prime. Then, for any choice of k, l , the following system of congruences:*

$$\begin{aligned}x &\equiv k \pmod a \\x &\equiv l \pmod b\end{aligned}$$

has a unique solution mod ab , i.e. it has solutions and any two solutions differ by a multiple of ab . In particular, there exists exactly one solution x such that $0 \leq x < ab$.

Proof. Let $x = k + ta$ for some integer t . Then x satisfies the first congruence, and our goal will be to find t such that x satisfies the second congruence.

To do this, write $k + ta \equiv l \pmod b$, which gives $ta \equiv l - k \pmod b$. Notice now that because a, b are relatively prime, a has an inverse $h \pmod b$ such that $ah \equiv 1 \pmod b$. Therefore $t \equiv h(l - k) \pmod b$, and $x = k + ah(l - k)$ is a solution to both the congruences.

To see uniqueness, suppose x and x' are both solutions to both congruences such that $0 \leq x, x' < ab$. Then we have

$$\begin{aligned}x - x' &\equiv k - k \equiv 0 \pmod a \\x - x' &\equiv l - l \equiv 0 \pmod b\end{aligned}$$

Thus $x - x'$ is a multiple of both a and b ; because a, b are relatively prime, this implies that $x - x'$ is a multiple of ab . Thus, any two solutions differ by a multiple of ab . \square

HOMEWORK

1. In the calendar used in many Asian countries, every year is associated with one of 12 animals (e.g. 2026 is the year of the Horse). Also, every year is associated with one of 5 elements: wood, fire, earth, metal, water (2026 is the year of fire).
Can you find the period of this calendar? I.e., in how many years will we return to the same animal and element?
2. (a) In one of the calendars used by Maya civilization, *Tzolkin*, each day is described by a number ranging 1–13 and a name (there are 20 names), e.g. 4 Ahau. Unlike our usual system of days in a month, when moving to the next day, both number and name are changed: e.g. if today is 1 Lamat, then tomorrow will be 2 Muluk.
What is the period of this calendar, i.e. after how many days will it start repeating?
(b) Maya used more than one calendar; the other calendar they used, called *Haab*, was 365 day cycle (unlike our calendar, there are no leap days). If we use this together with Tzolkin, what is the period of the combined calendar?
3. Assume that $\gcd(a, b) = d$. Let $a' = a/d, b' = b/d$. Show that then numbers a', b' are relatively prime, and deduce from that that any common multiple of a, b is a multiple of $da'b'$.
4. Use the previous problem to show that for any positive integers a, b we have $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.
5. Solve the following systems of congruences
 - (a)

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \end{aligned}$$
 - (b)

$$\begin{aligned} z &\equiv 1 \pmod{5} \\ z &\equiv 6 \pmod{7} \end{aligned}$$
6. Daniil has number of toys. If he tries to divide them equally among 4 kids, one toy is left over. Same happens if he tries to divide them equally among 5 or 6 kids; however, the toys can be divided equally among 7 kids. What is the smallest number of toys Daniil can have? [Hint: if number of toys is n , then what can you say about number $n - 1$?]
7. (a) Find the remainder upon division of 23^{2021} by 7.
(b) Find the remainder upon division of 23^{2021} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]
8. (a) Find the remainder upon division of 24^{46} by 100.
(b) Determine all integers k such that $10^k - 1$ is divisible by 99.