**MATH 8: HANDOUT 24**
**NUMBER THEORY 6: APPLICATIONS AND SUMMARY SO FAR**

## APPLICATION: CHECK DIGITS

An interesting application of congruences is so-called check digits. They are used to detect (but not correct) errors appearing when manually copying or entering long strings of numbers such as bank account numbers, credit card numbers, and more. Here is one application; UPC codes.

A Universal Product Code (UPC) is a numeric code assigned to virtually all products sold in stores; you usually see it as a bar code, which you scan at the cash register. The UPC is a 12-digit numeric code $a_1 \dots a_{12}$; the 12 digits have to satisfy the condition below:

$$3a_1 + a_2 + 3a_3 + a_4 + \cdots + a_{12} \equiv 0 \mod 10$$

The sum $3a_1 + a_2 + 3a_3 + a_4 + \cdots + a_{12} \mod 10$ is called the *checksum*.

If the digits do not satisfy this condition, it can not be a valid UPC code — so probably there was an error when scanning the barcode and it needs to be re-scanned. For example, 380177-051136 is a valid UPC code (check!); however, if the first 3 was replaced by 8, this would change the checksum by $3 \times 5 = 15 \equiv 5 \mod 10$, so the new checksum won't be zero.

It is easy to show that the UPC code always detects an error in single digit (this uses that 3 is invertible mod 10). It can also detect some (but not all) digit transpositions: e.g. if we replaced 380... by 308..., it would change the checksum:

old: $3 \times 3 + 8 + 3 \times 0 + \cdots = 17 + \cdots \equiv 7 + \dots$

new: $3 \times 3 + 0 + 3 \times 8 + \cdots = 33 + \cdots \equiv 3 + \dots$

## SUMMARY OF PREVIOUS RESULTS

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

**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

$$ax \equiv b \mod n$$

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

## HOMEWORK

When doing this homework, be careful that you only used the material we had proved or discussed so far — in particular, please do not use the prime factorization. And I ask that you only use integer numbers — no fractions or real numbers.

**1.** Is it true that the UPC code always detects transposition of two adjacent digits? Hint: suffices to consider how the checksum changes when we swap first and second digit, i.e. replace $ab\dots$ by $ba\dots$. How does this change the checksum?

**2.** In the calendar used in many Asian countries, every year is associated with one of 12 animals (e.g. 2021 is the Year of the Ox). Also, every year is associated with one of 5 elements: wood, fire, earth, metal, water (2021 is the year of metal).

Can you find the period of this calendar? I.e., in how many years will we return to the same animal and element?

**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 $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$.