J Kohonen

6B Number theory

6B1 (Parity) Early on the course we defined *even* and *odd* integers, both by *existential* statements:

$$n \text{ is even} \iff \exists k \in \mathbb{Z} : n = 2k$$
$$n \text{ is odd} \iff \exists k \in \mathbb{Z} : n = 2k + 1$$

Straight from these definitions, it is not obvious that these two are negations of each other (recall that by de Morgan, $\neg\exists\ldots$ is equivalent to $\forall\neg\ldots$). In fact there *are* numbers for which both statements are false (e.g. 2.5) so it seems this is a peculiar property of *integers*.

(a) Prove that if n is an integer, it cannot be both even and odd.

(b) Prove by induction that if $n \in \mathbb{N}$, then it is either even or odd. (Hint: Take 0 and 1 as base cases.)

(c) Prove that if $n \in \mathbb{Z}$, then it is either even or odd.

6B2 (Modulus operation) The *modulus* (or *remainder*) of $a \in \mathbb{Z}$, when dividing by $b \in \mathbb{Z}$, is the *smallest* element of the set

$$S = \{a - kb \ : \ k \in \mathbb{Z} \ \land \ a - kb \geq 0\}.$$

It is written $a \bmod b$, and by definition it is always a nonnegative integer. An intuitive explanation is that we look at all multiples of b (that is, numbers kb), and take the *biggest* of them that does not exceed a. Then take the difference $a - kb$, which is automatically nonnegative because of the way we defined it. Note that here mod is treated as an arithmetical *operation*, whose result is an integer.

In the following problems, a and b are integers.

(a) Find $123 \bmod 100$.

(b) Find $(-123) \bmod 100$.

(c) What is $a \bmod 2$ when a is even?

(d) What is $a \bmod 2$ when a is odd?

(e) What is $a \bmod 1$?

(f) What are the possible values of $a \bmod 3$?

(g) Prove or disprove: $a - (a \bmod b)$ is divisible by b. Give an example or a counterexample.

(h) Prove or disprove: $(a + b) \bmod c = (a \bmod c) + (b \bmod c)$. Give an example or a counterexample.

6B3 (Congruence) Two integers a, b are said to be *congruent modulo* n if $n \mid (b-a)$. It is written

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

(sometimes without parentheses). Note that congruence is a *relation* between numbers a and b. Also there is nothing preventing from one or both being negative: $9 \equiv -1 \pmod{10}$.

If we have a big bunch of congruences, all with the same modulus n, we often write simply

$$a \equiv b$$

and perhaps clarify just once that "all of these are mod n".

Prove or disprove each of the following (all are mod n, and a, b, c, d are integers). For true statements give a simple example. For false statements give a simple counterexample.

(a) $a \equiv a$.

(b) $(a \equiv 0) \iff (n \mid a)$.

(c) If $a \equiv b$ and $c \equiv d$, then $a + c \equiv b + d$.

(d) If $a \equiv b$ and $c \equiv d$, then $ac \equiv bd$.

(e) If $a \equiv b$, then $a^2 \equiv b^2$.

(f) If $a^2 \equiv b^2$, then $a \equiv b$.

(g) If $n = 2$ and $a^2 \equiv b^2$, then $a \equiv b$.

(h) If $a \equiv -1$, then $a^2 \equiv 1$.

(i) If $a^2 \equiv 1$, then $a \equiv 1$ or $a \equiv -1$. (Hint: Consider $n = 8$.)

(j) If $ab \equiv 0$, then $a \equiv 0$ or $b \equiv 0$.

Some of these statements show that congruences are a bit similar to identities, but not in all respects. If in doubt, always recall what a congruence really says (divisibility of the difference of LHS and RHS).

6B4 (Powers)

(a) When is $2^k \equiv 1 \pmod{3}$, if $k \in \mathbb{N}$?

(b) When is $3^k \equiv 1 \pmod{10}$, if $k \in \mathbb{N}$?

6B5 (Practical divisibility) When integers are written in the usual ten-based notation, some divisibility questions are easy even without performing a division. Note that if a is a nonnegative integer, then $(a \bmod 10)$ is its last digit, and $(a \bmod 100)$ are its last two digits.

Prove or disprove the following. For false statements give a counterexample. For true statements, give also an example of a where both sides of the equivalence are true, and a is bigger than 100.

(a) $2 \mid a$ if and only if $2 \mid (a \bmod 10)$.

(b) $3 \mid a$ if and only if $3 \mid (a \bmod 10)$.

(c) $4 \mid a$ if and only if $4 \mid (a \bmod 10)$.

(d) $4 \mid a$ if and only if $4 \mid (a \bmod 100)$.

(e) $5 \mid a$ if and only if $5 \mid (a \bmod 10)$.

6B6 (Last digits) Calculate the last two digits of 2024^{2024}.

Hint: Start by studying small powers of 2024 and try to argue how the sequence continues.

6B7 (Diophantine equations) Do the following Diophantine equations have solutions $x, y \in \mathbb{Z}$? If yes, find all solutions. If not, justify your answer.

(a) $20x + 10y = 65$

(b) $3x + 6y = 7$

(c) $20x + 16y = 500$