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.

Solution. a) Suppose n is both even and odd, then $n = 2x$ but also $n = 2y + 1$.

As x and y are both integers, so should be their difference, but instead we get the following contradiction.

$2x = 2y + 1 \to 1 = 2(x - y) \to \frac{1}{2} = x - y$

b) For the base case $n = 1 = 2k + 1, k = 0$ is odd and $n = 0 = 2k, k = 0$ is even. Our induction assumption is that n is either even or odd. Induction step has two cases:

Odd $n = 2k + 1 \to n + 1 = 2k + 2 = 2(k + 1)$ so $n + 1$ is even.

Even $n = 2k \to n + 1 = 2k + 1$ so $n + 1$ is odd. In both cases the induction step gives n that is either even or odd.

c) In b) we showed this for integers ≥ 0. For the negative integers consider even $-n = 2k \to n = -2k$ and odd $-n = 2k + 1 \to n = -2k - 1$. The same induction argument as in b) works; even becomes odd and odd becomes even.

Odd $n + 1 = -2k - 1 = -2k$ so $n + 1$ is even.

Even $n + 1 = -2k + 1 = -2\ell - 1$ for $\ell = k - 1$ so $n + 1$ is 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

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

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 mod 100.

(b) Find (-123) mod 100.

(c) What is a mod 2 when a is even?

(d) What is a mod 2 when a is odd?

(e) What is a mod 1?

(f) What are the possible values of a mod 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.

Solution.

a) $123 \bmod 100 = 23$
b) $-123 \bmod 100 = 77$
c) 0, since $2|a$ meaning there is $k \in Z$ such that $a = 2k$.
d) 1, since $a = 2k + 1$.
e) 0, since 1 divides all integers.
f) $0, 1, 2$
g) Is divisable. $a - (a \bmod b) = a - (a - kb) = kb, k \in Z$. For an example $5 - (5 \bmod 3) = 5 - 2$ giving $3 \mid 3$.
h) Not true. For example $(3 + 3) \bmod 2 = 0 \neq 2 = 3 \bmod 2 + 3 \bmod 2$.

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).

Solution.
a) True since $a - a = 0$ and $n \mid 0$.
b) True, $n \mid a \to n \mid (a - 0)$ so by definition $a \equiv 0$. Other direction: $a \equiv 0$ gives $n \mid (a - 0) \to n \mid a$.
c) True, write $a = b + kn$ and $c = d + \ell n$
$\to a + c = b + d + (k + \ell)n \equiv b + d$.
d) True, $ac = bd + b\ell n + dkn + k\ell n^2 \equiv bd$.
e) True, as above but $a = c$ and $b = d$.
f) False, for example $a = 4, b = 8, n = 16$ then $a^2 \equiv b^2 \equiv 0$ but $a \equiv 4$ and $b \equiv 8$.
g) True, since $1^2 = 1$ and $0^2 = 0$ are the only squares.
h) True, since $(-1 + nk)^2 = 1 - 2nk + n^2k^2 \equiv 1$.
i) False, for example $3^2 \equiv 1 \mod 8$.
j) False, for example $2^2 \equiv 0 \mod 4$. This would only be true when n is prime.

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 $k \in \mathbb{N}$?

Solution. a) When 2 has an even exponent $k = 2n$. $2^{2n} = 4^n \equiv 1$. $2^{2n+1} = 2 \cdot 4^n \equiv 2$.
b) When $k = 4n$. $3^{4n} = 81^n \equiv 1$. 3 and 10 are coprime so other powers have a different result.

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 $5 \mid (a \bmod 10)$.

Solution. a) True. $a \mod 10 = a - 10k = a - 2 \cdot 5k, k \in Z$. So if $2 \mid (a \mod 10)$ it follows that $2 \mid a$ and vice versa. An example: $102 \mod 10 \equiv 2$ and $2 \mid 2$ as well as $2 \mid 102$.

b) False, for example $3|27$ but does not divide 7.

c) False, for example $4|16$ but does not divide 6.

d) True, $a - 100k = a - 4 \cdot 25k$. An example: $240 \mod 100 \equiv 40$ and $4 \mid 40$ as well as $4 \mid 240$.

e) True, $a - 10k = a - 5 \cdot 2k$. An example: $515 \mod 10 \equiv 5$ and $5 \mid 5$ as well as $5 \mid 515$.

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.

Solution.

Work in $\mod 100$. The power in mod 100 can be written as $2024 \cdot ... \cdot 2024 \equiv 24 \cdot ... \cdot 24$. Computing the first products we get $24 \cdot 24 \equiv 76$ and $76 \cdot 24 \equiv 24$. We see that the result alternates between 24 for odd powers and 76 for even powers. 2024 being an even power means that $2024^{2024} \equiv 76$.

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) $20x + 16y = 500$

Solution.

a) $2(10x + 5y)$ is an even number thus can't equal 65.

b) $3(x + 2y) = 7$. No solutions since 3 does not divide 7.

c) $4(5x+4y) = 500 \rightarrow 5x+4y = 125 \rightarrow x = 125 - \frac{4}{5}y$. Then y must be a multiple of 5, $y = 5k$ which gives $x = 25 - 4k$.