EXERCISE SET 6,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

Explorative exercises

I recommend that you study the explorative problems before the first lecture of the week.

Recall that an integer $a \in \mathbb{Z}$ *divides* $b \in \mathbb{Z}$ ($a|b$) if there is $n \in \mathbb{Z}$ such that $an = b$.

Problem 1. To practice your understanding of the divisibility definition and of logical symbols, detemine whether the following statements are true or false. (All quantifiers are taken over the integers $\mathbb{Z}$.)

a) $\forall a : a|a$.
b) $\forall a : 1|a$.
c) $\forall a : a|1$.
d) $\forall a : 0|a$.
e) $\forall a : a|0$.
f) $\forall a, b : a|b \to b|a$.
g) $\forall a, b, c : (a|b \wedge a|c) \to a|b + c$.
h) $\forall a, b, c : (a|b \wedge b|c) \to a|c$.
i) $\forall a, b : (a|b \wedge b|a) \to (a = b \vee a = -b)$.

Problem 2. List all the integers that divide 98. Do the same with all numbers that divide 105. What is the *greatest common divisor* of 98 and 105?

Problem 3. The method used in Problem 2 to find the greatest common divisor is very inefficient if the numbers involved are large. Already computing, for example, $\gcd(2331, 2037)$ with this method seems like a disturbingly slow task. We will now find an easier algorithm to do this:

a) Show that, if $a, b, n \in \mathbb{Z}$, then the common divisors of a and b are the same as the common divisors of a and $b - na$.
b) Conclude that

$$\gcd(2331, 2037) = \gcd(2037, 2331 - 2037) = \gcd(2037, 294).$$

c) Continue this process, replacing $\gcd(2331, 2037)$ by the greatest common divisors of smaller and smaller numbers.
d) Show that, if $a > 0$, then $\gcd(a, 0) = a$.
e) Use this to compute $\gcd(2331, 2037)$.

Problem 4. Study the equation

$$3x - 2y = 1.$$

Clearly, it has the integer solution $x = 1, y = 1$.

a) Can you find more integer solutions? (Hint: if you add 2 to the value of x, how can you modify the value of y to get a new solution of the equation?)
b) Can you find *all* integer solutions? (And can you prove that there are no others?)

Homework

The written solutions to the homework problems should be handed in on MyCourses by Monday 11.4., 12:00. You are allowed and encouraged to discuss the exercises with your fellow students, but everyone should write down their own solutions.

Problem 1. (10pts) Does the following Diophantine equation

$$20x + 10y = 65.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Problem 2. (10pts) Does the following Diophantine equation

$$20x + 16y = 500.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Problem 3. (10pts) How many integers less than 22220 are relatively prime to 22220?

Problem 4. (10pts) Compute the last two digits of 2022^{2022}.

Additional problems

These do not need to be returned for marking.

Problem 1. Show that $7|13^n - 6^n$ for all $n \in \mathbb{Z}$.

Problem 2. Compute

a) $3^{19} \mod 13$.
b) $4^{12} \mod 27$.
c) $12^{27} \mod 15$.
d) $146^2 \mod 21$

Problem 3. Are the following statements true or false for arbitrary integers a, b, and n? Prove or find a counterexample.

a) If $a \equiv b \mod n$, then $a^2 \equiv b^2 \mod n$.
b) If $a^2 \equiv b^2 \mod n$, then $a \equiv b \mod n$.

Problem 4. Show that

$$144|n^8 - 2n^6 + n^4$$

for any integer n. (Hint: Factorize!)

Problem 5. Compute

a) $\varphi(200)$.
b) $\varphi(121)$.
c) $\varphi(635)$.
d) $\varphi(1010)$.
e) $\varphi(2021)$.

where φ denotes Euler's phi function.

Problem 6. A seemingly very difficult open question in number theory is whether there are infinitely many "twin primes", meaning two consecutive odd numbers that are both primes. Show that there are only finitely many (in fact, only one "triplet prime"), meaning *three* consecutive odd numbers that are all primes.

Exercise 7 (challenging). Let F_n be the n:th Fibonnacci number.

a) Prove that $\gcd(F_n, F_{n-1}) = 1$.
b) How many steps does Euclid's algorithm take to compute $\gcd(F_n, F_{n-1})$?
c) Show that, if a, b are any numbers with $b \leq a < F_n$, then Euclid's algorithm requires more steps to compute $\gcd(F_n, F_{n-1})$, than to compute $\gcd(a, b)$. (Punchline: The Fibonnacci numbers are the worst possible input for Euclid's algorithm.)