HOMEWORK 04, DUE BY 2022-02-12

Question 1: Let $\mathbb{Z}_n$ denote the set of all congruence classes modulo n. For each function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ find the *cardinality of the range* of f – namely, the count of elements $y \in \mathbb{Z}_n$ that can be values $f(x)$ for some $x \in \mathbb{Z}_n$. Provide brief explanations for your answers.

(A) $f_1\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_1(n) = (18n + 5) \bmod 41$.

(B) $f_2\colon \mathbb{Z}_{44} \to \mathbb{Z}_{44}$ defined by $f_2(n) = (18n + 5) \bmod 44$.

(C) $f_3\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_3(n) = n^5 \bmod 41$.

(D) $f_4\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_4(n) = 5^n \bmod 41$.

(E) $f_5\colon \mathbb{Z}_{49} \to \mathbb{Z}_{49}$ defined by $f_5(n) = 5^n \bmod 49$.

Question 2:

(A) Find $\gcd(\gcd(\gcd(81719, 52003), 33649), 30107)$ showing the steps of Euclidean algorithm.

(B) Let $\gcd(a, b, c)$ be the *greatest common divisor* of 3 numbers $a, b, c \in \mathbb{Z}^+$ – the largest $d \in \mathbb{Z}^+$ such that $d \mid a$, and $d \mid b$, and $d \mid c$. Prove that any integer m divides $\gcd(a, b, c)$ iff m divides $\gcd(\gcd(a, b), c)$.

(C) Prove that $\gcd(a, b, c) = d$ is the smallest positive integer obtainable in the form $d = ax + by + cz$, where $x, y, z \in \mathbb{Z}$. (*Hint:* Apply Bézout's identity repeatedly.)

Question 3:

(A) How many integers between 1 and 1000 inclusive has a remainder 1 when divided by 7 and a remainder 3 when divided by 4?

(B) Write a formula (depending on the parameter n) to find the count of integer solutions $x \in [1; n]$ to the following system:

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{4} \end{cases}$$

(C) Find the smallest positive integer that has a remainder 5 when divided by 7, a remainder of 6 when divided by 11, and a remainder of 4 when divided by 13.

(D) Write an expression (depending on parameters a, b, c) to compute the smallest positive integer x that is the solution of the system of congruences:

$$\begin{cases} x \equiv a \pmod{7} \\ x \equiv b \pmod{11} \\ x \equiv c \pmod{13} \end{cases}$$

Note: Formulas in (B), (D) may use arithmetic operations, the floor ($\lfloor x \rfloor$), the ceiling $\lceil x \rceil$, integer division ($k \operatorname{div} \ell$), and remainder ($k \bmod \ell$). For modular multiplicative inverses see https://bit.ly/348GVqJ.

Question 4: Translate every predicate expression in plain English, use number theory concepts whenever possible. Prove or disprove the statements.

Predicate $m \mid n$ is true iff m divides n; predicate $\textsc{isPrime}(p)$ is true iff p is a prime.

(A) $\exists a_0 \in \mathbb{N}\, \exists d \in \mathbb{N} \left(d > 0 \land \forall k \in \mathbb{N}\, \forall m \in \mathbb{N} \left((m \mid (a_0 + k \cdot d)) \to (m = 1 \lor m = a_0 + k \cdot d) \right) \right)$.

(B) $\forall p \in \mathbb{N}\, \exists a \in \mathbb{N}\, ((\textsc{isPrime}(p) \land \neg(2 \mid p)) \to a \neq 1 \land a^{\frac{p-1}{2}} \equiv 1 \pmod{p})$.

(C) $\forall k \in \mathbb{N} \left(k \geq 2 \to \forall n \in \mathbb{N}\, \forall j \in \mathbb{N} \left(j < k \to \forall m \in \mathbb{N} \left((1 < m \land m < k) \to \neg(m \mid (n + j)) \right) \right) \right)$.

Question 5:

(A) List all integers $n \in [1; 90]$ such that $\gcd(n, 90) = 3$.

(B) Prove that for every positive integer $m \in \mathbb{Z}^+$, and for every positive integer d such that $d \mid m$ we have

$$\left| \{ x \in \mathbb{Z}^+ \mid x \leq m \land \gcd(x, m) = d \} \right| = \varphi(m/d).$$

Question 6:

Introduction: Miller-Rabin primality test is a probabilistic algorithm to find, if a number is prime. It is the most popular primality test in libraries such as Python's `sympy.isprime(n)`. The documentation of `sympy` package says that for $n < 2^{64}$ the answer is always correct, but for larger values n there is a probability that the algorithm will lie and identify some non-prime as a prime (false positive). Miller-Rabin primality test does not have false negatives – if it outputs the answer that the number is composite, this means that a *witness* has been found, which proves that it is definitely composite.

$\textsc{Witness}(a, n)$:
- express $n - 1 = 2^t u$, where u is odd.
- $x_0 = a^u \bmod n$
- **for** i **in** $\textsc{range}(0, t)$: (*repeat t times*)
    - $x_i = x_{i-1}^2 \bmod n$
    - **if** $x_i == 1$ **and** $x_{i-1} \neq 1$ **and** $x_{i-1} \neq n - 1$
        - **return** TRUE (*evidence that n is definitely composite*)
- **if** $x_t \neq 1$
    - **return** TRUE (*evidence that n is definitely composite*)
- **return** FALSE

$\textsc{MillerRabin}(n, s)$:
- **for** j **in** $\textsc{range}(1, s + 1)$
    - let a be a random number from $\{1, 2, \ldots, n - 1\}$
    - **if** $\textsc{Witness}(a, n)$
        - **return** COMPOSITE (*definitely composite*)
- **return** PRIME (*very likely prime*)

To improve the probability of correct answer from Miller-Rabin algorithm one can increase the number of witness-probes – the parameter s in the above pseudocode. How do we know, which value s is sufficient? It may happen that the chance to get a wrong answer depends on the number n being tested. In this problem you will find out which composite numbers n are most likely to lead to wrong answers from this primality test.

Problem: Consider the set of positive integers $S = \{n \in \mathbb{Z}^+ \mid 2 \leq n \leq 2000\}$. Find those three integers $n_1, n_2, n_3 \in S$ which have the *highest* probabilities that the function $\textsc{Witness}(a, n)$ for a random $a \in \{1, 2, \ldots, n_i - 1\}$ will fail to determine that n_i is a composite number (even though it is in fact composite).

For each of the three numbers indicate the total number of "false witnesses" (those a for which $\textsc{Witness}(a, n)$ does not produce evidence that n_i was composite). Also compute the probability to get a false witness as a rational fraction. (It may be useful to use computing devices to find the most risky composite numbers up to 2000.)

Example: If we pick $n = 21$, then for $a \in \{1, 8, 13, 20\}$ we fail to produce a witness that $n = 21$ is composite. Indeed, express $n - 1 = 20 = 5 \cdot 2^2$ ($t = 2$, $u = 5$).

Raising all the numbers $a \in \{1, 8, 13, 20\}$ to the power $u = 5$ (Line 2 in the algorithm $\textsc{Witness}(a, n)$) we get the following results:

$$\begin{cases} 1^5 \equiv 1 \pmod{21} \\ 8^5 \equiv 8 \pmod{21} \\ 13^5 \equiv 13 \pmod{21} \\ 20^5 \equiv 20 \pmod{21} \end{cases}$$

Squaring any of these numbers exactly $t = 2$ times would be congruent to 1 modulo 21. Thus these numbers $a \in \{1, 8, 13, 20\}$ create a false impression that $n = 21$ satisfies the Little Fermat theorem since $a^{n-1} \equiv 1 \pmod{n}$. Other values $a \in [1; 20]$ are fine as witnesses and produce correct evidence that $21 = 3 \cdot 7$ is a composite number.

Thus for $n = 21$ the probability of a "false witness" in $\textsc{Witness}(a, n)$ for a single randomly chosen a is $P_{21} = \frac{4}{20} = \frac{1}{5}$. In your answer find those $n_1, n_2, n_3 \leq 2000$ which have the three highest probabilities $P_{n_1}, P_{n_2}, P_{n_3}$ to pick a false witness.