NUMBER THEORY: HOMEWORK 4

TO BE HANDED IN BY WEDNESDAY 20TH SEPTEMBER 2023

1. (i) Find an integer x such that $3x \equiv 2 \pmod{5}$, $2x \equiv 3 \pmod{23}$, and $7x \equiv 5 \pmod{3}$. Find an infinite sequence of integers with the same property.

(ii) Find an integer x such that $3x \equiv 2 \pmod{7}$, $5x \equiv 3 \pmod{19}$, and $7x \equiv 5 \pmod{9}$. Find an infinite sequence of integers with the same property.

(iii) Find all integers x satisfying $2x \equiv 7 \pmod{15}$ and $5x \equiv 17 \pmod{33}$.

2. (i) Find solutions of $x^2 \equiv -1 \pmod{5}$ and $x^2 \equiv -1 \pmod{13}$. Hence, applying the Chinese Remainder Theorem, obtain a solution of $x^2 \equiv -1 \pmod{65}$.

(ii) How many solutions does $x^2 \equiv -1 \pmod{65}$ possess?

3. (i) Let p be a prime number. By applying Fermat's Little Theorem, or otherwise, show that the congruence $x^p - x + 1 \equiv 0 \pmod{p}$ has no solution.

(ii) How many solutions does the congruence $x^{16} - x + 3 \equiv 0 \pmod{40}$ possess? Explain your answer.

4. By considering the prime factorisation of the integer 1729, prove that whenever $(a, 1729) = 1$, one has $a^{36} \equiv 1 \pmod{1729}$. Hence prove that $a^{1728} \equiv 1 \pmod{1729}$ whenever $(a, 1729) = 1$.

5. (i) Recall that if p is prime and $x^2 + 1 \equiv 0 \pmod{p}$ is soluble, then $p = 2$ or $p \equiv 1 \pmod{4}$. By modifying Euclid's proof that there are infinitely many primes, deduce that there are infinitely many primes of the form $4k+1$ ($k \in \mathbb{N}$).

(ii) Show that there are infinitely many primes of the form $8k + 5$ ($k \in \mathbb{N}$).