Math 211

Assignment 5

Due 5 November 2021

[2] 1. Consider the following statements about integers x and y:

(a) $3x \equiv 3y \pmod{17} \quad \Rightarrow \quad x \equiv y \pmod{17}$;

(b) $3x \equiv 9y \pmod{15} \quad \Rightarrow \quad x \equiv 3y \pmod{15}$;

For each of the above statements, decide whether it is true or false. If it is true, explain why (by using a suitable theorem). If it is false, give a counterexample, i.e. find explicit values of x and y for which the statement is false (and explain why these values show that it is false).

[3] 2. (a) Prove that $x^2 \equiv 0, 1,$ or $4 \pmod{8}$, for any integer $x \in \mathbb{Z}$.

(b) Show that number of the form $n = 8k + 7$ can never be the sum of three squares; in other words, $n \neq x^2 + y^2 + z^2$, for any $x, y, z \in \mathbb{Z}$.

[5] 3. Find all the solutions of the following congruences:

(a) $11x \equiv 23 \pmod{57}$;

(b) $12x \equiv 28 \pmod{63}$;

(c) $16x \equiv 40 \pmod{36}$.

[2] 4. Solve each of the following equations in the given field or ring.

(a) $5x = 2$ in $\mathbb{F}_{13}$;

(b) $16x = 40$ in $\mathbb{Z}/36\mathbb{Z}$;

[5] 5. In each case, use the Chinese Remainder Theorem to find the smallest positive integer x which satisfies the indicated simultaneous congruences:

$$\text{(a)} \quad \begin{array}{rcll} x & \equiv & 11 & \pmod{27} \\ x & \equiv & 13 & \pmod{31} \end{array} \qquad\qquad \text{(b)} \quad \begin{array}{rcll} x & \equiv & 3 & \pmod{21} \\ x & \equiv & 4 & \pmod{26} \\ x & \equiv & 5 & \pmod{31} \end{array}$$

[3] 6. Maple Probem: (a) Compute rem($12345^{123456789}$, 7777) by using both MAPLE's power-mod command (i.e. `Power(a,n) mod m`) and by the naive method (using `irem(a^n, m)`). Comment on which method is better (and why).

(b) Recall that in order to apply the power-mod algorithm given in class, we need to know the binary digits of the exponent n. In MAPLE, this can be done in two ways: either by finding the binary expansion of n by using the command `convert(n, binary)` or by finding the list of binary digits of n (in its binary expansion) via the command `convert(n, base, 2)`. Use these commands to find the binary expansion and the list of binary digits for $n = 500$. Interpret the output (and check that this is correct) by writing it in the form used in class: $n = 2^r + i_1 2^{r-1} + \ldots + i_r$