MATH 311, FALL 2024 MIDTERM 1

SEPTEMBER 25

Each problem is worth 10 points.

Problem 1.

a. State the Chinese Remainder Theorem.
b. Find an integer n that satisfies the congruences $n \equiv 1 \bmod 4$, $n \equiv 2 \bmod 5$, $n \equiv 7 \bmod 11$.

Solution.

a. Given a system of congruences $a_i \bmod m_i$ to co-prime moduli $m_1, ..., m_k$ there exists a unique $a \bmod m$, $m = m_1 \cdots m_k$ so that $a \equiv a_i \bmod m_i$ for each i. The solution may be found as $a \equiv \sum_i a_i b_i \frac{m}{m_i}$ where $b_i \cdot \frac{m}{m_i} \equiv 1 \bmod m_i$.
b. 117 is a solution. One way of arriving at this is to notice $20 \cdot 5 \equiv 1 \bmod 11$, $44 \cdot 4 \equiv 1 \bmod 5$ and $55 \cdot 3 \equiv 1 \bmod 4$, and $7 \cdot 20 \cdot 5 + 2 \cdot 44 \cdot 4 + 1 \cdot 55 \cdot 3 = 1217 \equiv 117 \bmod 220$.

Problem 2.

a. State the Euclidean algorithm.
b. Using the Euclidean algorithm or otherwise find $g = \mathrm{GCD}(91, 1001)$ and find integers x, y so that $91x + 1001y = g$.

Solution. a. Given two non-zero integers a, b with $a > b > 0$, form a sequence $x_1 = a, x_2 = b$, and given $x_{n-1} > x_n > 0$, $x_{n-1} = qx_n + x_{n+1}$ where $0 \leq x_{n+1} < x_n$ as in the division algorithm. The sequence stops at the first n for which $x_n = 0$ and the gcd of a and b is then x_{n-1}.

b. Since $1001 = 91 \cdot 11$, the gcd of 91 and 1001 is 91. We have $91 = 1 \cdot 91 + 0 \cdot 1001$.

Problem 3. State Fermat's Little Theorem and give a proof.

Solution. If p is prime and $(a,p) = 1$, $a^{p-1} \equiv 1 \bmod p$ and $a^p \equiv a \bmod p$ for all $a \bmod p$. For general $m > 0$ and $(a,m) = 1$, $a^{\phi(m)} \equiv 1 \bmod m$. The first statement follows from the second for general m since if p is prime, $\phi(p) = p - 1$. For general m the proof is as follows. Let $x_1, x_2, ..., x_{\phi(m)}$ be a reduced residue system modulo m. Then $ax_1, ..., ax_{\phi(m)}$ are all co-prime to m, and are not congruent, since a has an inverse modulo m. It follows that $ax_1, ..., ax_{\phi(m)}$ is again a reduced residue system modulo m, so that each congruence class $x_i \bmod m$ occurs exactly once among $ax_1, \cdots, ax_{\phi(m)}$. Thus

$$x_1 \cdots x_{\phi(m)} \equiv (ax_1) \cdots (ax_{\phi(m)}) \equiv a^{\phi(m)} x_1 \cdots x_{\phi(m)} \bmod m.$$

Multiplying both sides by the inverse of $x_1 \cdots x_{\phi(m)}$ obtains $a^{\phi(m)} \equiv 1 \bmod m$.

Problem 4. Find a primitive root modulo $343 = 7^3$.

Solution. We show 3 is a primitive root modulo 7^3. We have $3^1 = 3, 3^2 = 9 \equiv 2 \bmod 7, 3^3 = 27 \equiv 6 \bmod 7, 3^4 = 81 \equiv 4 \bmod 7, 3^5 = 243 \equiv 5 \bmod 7, 3^6 = 729 \equiv 1 \bmod 7$. Since these are all distinct, 3 is a primitive root mod 7. Since $3^6 \equiv 43 \not\equiv 1 \bmod 49$, the order of 3 mod 49 is not 6, but it can only be 6 or $\phi(49) = 42$ so it must be 42, and hence 3 is a primitive root mod 49. Since it is a primitive root mod $49 = 7^2$ it is a primitive root mod $343 = 7^3$.