115 Homework 7 Solutions

Due Friday November 19

Question 1 (Midterm *déja vu*.) Prove that the system of congruences

$$x \equiv a_1 \text{ mod } m_1 , ... , x \equiv a_r \text{ mod } m_r ,$$

has a unique solution modulo $m_1 \dots m_r$ when $m_1, \dots, m_r$ are pairwise relatively prime.

Solution Let $M = m_1 m_2 \cdots m_r$ and $M_k = M/m_k$. Now we see that $x = a_1 M_1 y_1 + \dots a_r M_r y_r$ where $M_k y_k \equiv 1$ (mod m_k) is indeed a solution since to the system of congruences since every summand of x has a factor of m_k except $a_k M_K y_k$ so that $x \equiv a_k M_k y_k \equiv a_k(1) \equiv a_k$ (mod m_k). Now we prove uniqueness: Assume there are 2 solutions, x and y to the above system of congruences. Then $x \equiv y \equiv a_k$ (mod m_k) for $k = 1, \dots, r$. This impies that $m_k|(x - y)$ for $k = 1, \dots, r$ and since all the m_k's are relatively prime we have that $m_1 m_2 \cdots m_r = M|(x - y) \Rightarrow x \equiv y$ (mod M). This shows that the solution x of the system of congruences is unique modulo M.

Question 2 (Rosen 6.1.10) What is the remainder when 6^{2000} is divided by 11?

Solution From Fermat's little theorem, we know that $6^{10} \equiv 1$ (mod11). Then $6^{2000} \equiv (6^{10})^{200} \equiv 1^{200} \equiv 1$ (mod 11). Therefore the remainder is 11.

Question 3 (Rosen 6.1.34) Show that if p is prime and $0 < k < p$, then

$$(p - k)!(k - 1)! \equiv (-1)^k \text{ mod } p\,.$$

Solution We have $(p - k)!(k - 1)! \equiv (-k)(-(k + 1)) \cdots (-(p - 1))(k - 1)! \equiv (-1)^{p-k}(p - 1)(p - 2) \cdots (k + 1)(k)(k - 1)! \equiv (-1)^{p+1-k} \equiv (-1)^k$ (mod p), by Wilson's theorem, and where we have used the fact that $p + 1$ is even.

Question 4 (Rosen 6.1.40,41) Utilize the fact that if p is prime and $0 < k < p$ then $p|\binom{p}{k}$ to show that integers a and b obey $(a+b)^p = a^p + b^p$ mod p. Now give an inductive proof of Fermat's little theorem.

Solution (40) We have $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \equiv a^p b^0 + 0 + 0 + \cdots + a^0 b^p \equiv a^p + b^p$ (mod p) since $\binom{p}{k} \equiv 0$ (mod p) for $1 \leq k \leq p-1$.

(41) We first note that $1^p \equiv 1$ (mod p). Now suppose $a^p \equiv a$ (mod p). Then from above we see that $(a+1)^p \equiv a^p + 1$ (mod p). But by the inductive hypothesis $a^p \equiv a$ (mod p) we see $a^p + 1 \equiv a + 1$ (mod p) . Hence $(a+1)^p \equiv a + 1$ (mod p). This completes the inductive step of the proof.

Question 5 (Rosen 6.2.2) Show 45 is pseudoprime base 17 and 19.

Solution Note that $17^4 \equiv 19^2 \equiv 1$ (mod 45). Then, $17^45 \equiv 17^{4 \cdot 11} 17 \equiv 1^{11} 17 \equiv 17$ (mod 45), and $19^{45} \equiv 19^{2 \cdot 22} 19 \equiv 1^{22} 19 \equiv 19$ (mod 45). So 45 is a pseudoprime to the bases 17 and 19.

Question 6 (Rosen 6.2.20) Show all Carmichael numbers are squarefree.

Solution Let n be a Carmichael number and suppose there is a prime p such that $n = p^t m$, with $(p, m) = 1$ and $t \geq 2$. Let $x = b$ be a solution to the system of congruences $x \equiv p^{t-1} + 1$ (mod p^t), $x \equiv 1$ (mod m). Then since $(b, p) = 1$ and $(b, m) = 1$, we have that $(b, n) = 1$. If it were the case that $b \equiv 1$ (mod n), then we would have $b \equiv 1$ (mod p^t), a contradiction. Therefore $b \not\equiv 1$ (mod n). On the other hand, note that $b^n \equiv (p^{t-1}+1)^n \equiv (p^{t-1})^n + n(p^{t-1})^{n-1} + \cdots + np^{t-1} + 1 \equiv 1$ (mod p^t), by the binomial theorem and the fact that $p|n$, so p^t divides every term but the last. Also $b^n \equiv 1$ (mod m), so that by the Chinese remainder theorem, we must have $b^n \equiv 1$ (mod n). Since $(b, n) = 1$ and $b \not\equiv 1 \equiv b^n$ (mod n), n is not a Carmichael number. Therefore n must be squarefree.