Math 110 Problem Set 2 Solutions

3.8 Let $p \geq 3$ be prime. Show that the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$.

Solution: Note that we have

\[(x + 1) \cdot (x - 1) \equiv x^2 - 1 \equiv 0 \pmod{p}\]

Thus, by Exercise 7(a), we have that either $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$ so we have $x \equiv \pm 1 \pmod{p}$ as required.

3.9 Suppose $x \equiv 2 \pmod{7}$ and $x \equiv 3 \pmod{10}$. What is $x$ congruent to mod 70?

Solution: This is easiest to do by trial and error. The 2nd condition means that $x$ is 3, 13, 23, 33, 43, 53, or 63 modulo 70. Checking, we see that the only one of these which is 2 modulo 7 is 23, so $x$ must be 23 (mod 70). Note that the Chinese Remainder Theorem guarantees that there is a unique answer to the question.

3.11 Let $p$ be prime. Show that $a^p \equiv a \pmod{p}$ for all $a$.

Solution: Let us consider two cases: $p$ divides $a$, and $p$ does not divide $a$. If $p$ divides $a$, then both sides are 0 modulo $p$. If $p$ does not divide $a$, by Fermat’s Little Theorem,

\[a^{p-1} \equiv 1 \pmod{p}\]

\[\Rightarrow a^p \equiv a \pmod{p}\]

Thus, in either case, $a^p \equiv a \pmod{p}$

3.12 Divide $2^{10203}$ by 101. What is the remainder?

Solution: Note that by Fermat’s Little Theorem, $2^{100} \equiv 1 \pmod{101}$. Thus, we have that for any integer $n$, $2^{100n} \equiv 1 \pmod{101}$, raising both sides to the power of $n$. Hence, we have that $2^{10200} \equiv 1 \pmod{101}$, so we conclude that

\[2^{10203} \equiv 2^3 \cdot 2^{10200} \equiv 8 \pmod{101}\]

Thus, the remainder from the division is 8.

3.15 (a) Compute $\phi(d)$ for all of the divisors of 10 (namely, 1, 2, 5, 10) and find the sum of all these $\phi(d)$.

(b) Repeat part (a) for all the divisors of 12.

(c) Let $n \geq 1$. Conjecture the value of $\sum \phi(d)$, where the sum is over the divisors of $n$. 

1
Solution:
(a) We calculate:
\[ \phi(1) = 1 \]
\[ \phi(2) = 2 - 1 = 1 \]
\[ \phi(5) = 5 - 1 = 4 \]
\[ \phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4 \]
Here we have used the fact that \( \phi(p) = p - 1 \) for a prime \( p \) and the formula for \( \phi(n) \) in the textbook. Thus, we have that the sum of all these is \( 1 + 1 + 4 + 4 = 10 \).

(b) We calculate:
\[ \phi(1) = 1 \]
\[ \phi(2) = 2 - 1 = 1 \]
\[ \phi(3) = 3 - 1 = 2 \]
\[ \phi(4) = 4 \times (1 - \frac{1}{2}) = 2 \]
\[ \phi(6) = \phi(2) \times \phi(3) = 1 \times 2 = 2 \]
\[ \phi(12) = 12 \times (1 - \frac{1}{2})(1 - \frac{1}{3}) = 2 \times 2 = 4 \]
Thus, we have that the sum of all these is \( 1 + 1 + 2 + 2 + 2 + 4 = 12 \).

(c) The previous two examples suggest that this sum is \( n \).

3.17
(a) Show that every nonzero congruence class mod 11 is a power of 2, and therefore 2 is a primitive root mod 11.
(b) Note that \( 2^3 \equiv 8 \pmod{11} \). Find \( x \) such that \( 8^x \equiv 2 \pmod{11} \).
(c) Show that every nonzero congruence class mod 11 is a power of 8, and therefore 8 is a primitive root mod 11.
(d) Let \( p \) be prime and let \( g \) be a primitive root mod \( p \). Let \( h \equiv g^y \pmod{p} \) with \( \gcd(y, p - 1) = 1 \). Let \( xy \equiv 1 \pmod{p - 1} \). Show that \( h^x \equiv g \pmod{p} \).
(e) Let \( p \) and \( h \) be as in part (d). Show that \( h \) is a primitive root mod \( p \).

Solution:   (a) Let us calculate the powers of 2 modulo 11:
\[ 2 \equiv 2 \pmod{11} \]
\[ 2^2 \equiv 4 \pmod{11} \]
\[ 2^3 \equiv 8 \pmod{11} \]
\[ 2^4 \equiv 16 \equiv 5 \pmod{11} \]
\[ 2^5 \equiv 2 \times 2^4 \equiv 2 \times 5 \equiv 10 \pmod{11} \]
\[ 2^6 \equiv 2 \times 2^5 \equiv 2 \times 10 \equiv 9 \pmod{11} \]
2^7 \equiv 2 \cdot 2^6 \equiv 2 \cdot 9 \equiv 7 \pmod{11}
2^8 \equiv 2 \cdot 2^7 \equiv 2 \cdot 7 \equiv 3 \pmod{11}
2^9 \equiv 2 \cdot 2^8 \equiv 2 \cdot 3 \equiv 6 \pmod{11}
2^{10} \equiv 2 \cdot 2^9 \equiv 2 \cdot 6 \equiv 1 \pmod{11}

Thus, we see that every congruence class mod 11 appears, so 2 is a primitive root mod 11.

(b) Note that the inverse of 3 (mod 10) is 7 (mod 10). Now, by Fermat’s Little Theorem, 2^{10} \equiv 1 (mod 11). Thus,

\begin{align*}
2^3 &\equiv 8 \pmod{11} \\
\Rightarrow (2^3)^7 &\equiv 8^7 \pmod{11} \\
\Rightarrow 8^7 &\equiv 2^{21} \equiv 2 \pmod{11}
\end{align*}

Thus, the x we want is 7.

(c) Let c be a congruence class mod 11. By (a), there exists x such that 2^x \equiv c (mod 11). Applying the formula from (b), we have that 8^{7x} \equiv c (mod 11). Thus every nonzero congruence class mod 11 is a power of 8.

(d) Since xy \equiv 1 \pmod{p-1}, by Fermat’s Little Theorem,

\begin{align*}
g^{x^y} &\equiv g \pmod{p} \\
\Rightarrow h^x \equiv (g^y)^x &\equiv g^{xy} \equiv g \pmod{p}
\end{align*}

(e) Let c be a congruence class mod p. Then, since g is a primitive root mod p, there exists a such that g^a \equiv c (mod p). Thus, we have that h^{ax} \equiv c (mod p), so every nonzero congruence class mod p is a power of h. Hence h is a primitive root mod p.