Solutions to Math 332 Homework 8

7. Note that (iii) actually follows immediately from definition.

(i) Given \( a \equiv b \pmod{p} \), we have
\[
\left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv \left( \frac{b}{p} \right) \quad \pmod{p}
\]
by Euler’s criterion. Since \((a/p), (b/p) \in \{-1, 1\}\) and \(p \neq 2\), it follows that \((a/p) = (b/p)\).

(ii) By Euler’s criterion,
\[
\left( \frac{ab}{p} \right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \quad \pmod{p}.
\]
Since \((ab/p), (a/p)(b/p) \in \{-1, 1\}\) and \(p \neq 2\), it follows that \((ab/p) = (a/p)(b/p)\).

(iii) By Euler’s criterion and Fermat’s theorem,
\[
\left( \frac{a^2}{p} \right) \equiv a^{p-1} \equiv 1 \quad \pmod{p}.
\]
Since \((a^2/p) \in \{-1, 1\}\), we must have \((a^2/p) = 1\).

(iv) This follows from (ii) and (iii)
\[
\left( \frac{a^2b}{p} \right) = \left( \frac{a^2}{p} \right) \left( \frac{b}{p} \right).
\]

8. Clearly \(2 \mid (n^2 - 2)(n^2 - 5)(n^2 - 40)\) for every \(n \in \mathbb{N}\) and \(5 \mid (n^2 - 2)(n^2 - 5)(n^2 - 40)\) for every \(n \in \{5k \mid k \in \mathbb{N}\}\). If \(p\) is a prime such that \(p \neq 2, 5\), then
\[
n^2 \equiv 2 \quad \pmod{p} \text{ for some } n \in \mathbb{N} \iff \left( \frac{2}{p} \right) = 1 \quad (1)
\]
\[
n^2 \equiv 5 \quad \pmod{p} \text{ for some } n \in \mathbb{N} \iff \left( \frac{5}{p} \right) = 1 \quad (2)
\]
\[
n^2 \equiv 40 \quad \pmod{p} \text{ for some } n \in \mathbb{N} \iff \left( \frac{40}{p} \right) = 1 \iff \left( \frac{2}{p} \right) = \left( \frac{5}{p} \right) \quad (3)
\]
Observe that if \((2/p) \neq (5/p)\), then either (1) or (2) must hold. So for any \(p \neq 2, 5\), (1) or (2) or (3) must hold, i.e., there exists some \(n_0 \in \mathbb{N}\) such that \(n_0^2 \equiv 2, 5\) or 40 \(\pmod{p}\). It then follows from binomial expansion that
\[
(n_0 + kp)^2 \equiv 2, 5 \text{ or } 40 \quad \pmod{p}
\]
for every \(k \in \mathbb{N}\). Hence \(p \mid (n^2 - 2)(n^2 - 5)(n^2 - 40)\) for every \(n \in \{n_0 + kp \mid k \in \mathbb{N}\}\).

9. (a) Check that 313 is prime. As before
\[
313 \mid n^2 - 3 \text{ for some } n \in \mathbb{N} \iff n^2 \equiv 3 \quad \pmod{313} \text{ for some } n \in \mathbb{N} \iff \left( \frac{3}{313} \right) = 1.
\]
Since 313 \(\equiv 1 \pmod{12}\), \(3/313 = 1\) by (5.13)(ii), it follows that \(n^2 \equiv 3\) is a multiple of 313 for some \(n \in \mathbb{N}\).
(b) Check that 97 is prime. As before

\[ 97 \mid n^2 + 3 \text{ for some } n \in \mathbb{N} \iff n^2 \equiv -3 \pmod{97} \text{ for some } n \in \mathbb{N} \iff \left( \frac{-3}{97} \right) = 1. \]

Since 97 \equiv 1 \pmod{6}, \left( \frac{-3}{97} \right) = 1 by (5.13)(iii), it follows that 97 \mid n_0^2 + 3 for some \( n_0 \in \mathbb{N} \), so 97 \mid n^2 + 3 for every \( n \in \{ n_0 + 3k \mid k \in \mathbb{N} \} \).

10. Let \( p \) be a prime and \( p \mid 4n^2 + 28n + 51 \) (so \( p \) is clearly odd). By (5.1),

\[ 4n^2 + 28n + 51 \equiv 0 \pmod{p} \iff \begin{cases} m^2 \equiv -32 \pmod{p} \\ 8n \equiv m - 28 \pmod{p}. \end{cases} \]

Since \( (8, p) = 1 \), the linear congruence is always solvable for any value of \( m \). So the system is solvable if and only if \( m^2 \equiv -32 \pmod{p} \) is solvable, ie.

\[ 1 = \left( \frac{-32}{p} \right) = \left( \frac{-2^5}{p} \right) = \left( \frac{-2}{p} \right) \]

which holds if and only if \( p \equiv 1, 3 \pmod{8} \), by (5.13)(i).

12. Clearly \( n^2 + 6 \) is divisible by 2 (resp. 3) if and only if \( n \) is divisible by 2 (resp. 3). If \( p \) is a prime, \( p \neq 2, 3 \), then

\[ n^2 + 6 \equiv 0 \pmod{p} \implies n^2 \equiv -6 \pmod{p} \implies \left( \frac{-6}{p} \right) = 1 \]

\[ \implies \left( \frac{2}{p} \right) \left( \frac{-3}{p} \right) = 1 \implies \left( \frac{2}{p} \right) = 1 = \left( \frac{-3}{p} \right) \text{ or } \left( \frac{2}{p} \right) = -1 = \left( \frac{-3}{p} \right) \]

\[ \implies \begin{cases} p \equiv \pm 1 \pmod{8} \\ p \equiv 1 \pmod{6} \end{cases} \text{ or } \begin{cases} p \equiv \pm 3 \pmod{8} \\ p \equiv -1 \pmod{6} \end{cases}. \]

(Note that \( (-3/p) = -1 \) gives only \( p \equiv -1 \pmod{6} \) because the cases \( p \equiv 2, 3, 4 \pmod{6} \) would imply \( p = 2, 3 \). So we obtain four sets of congruence relations

\[ \begin{cases} p \equiv 1 \pmod{3} \\ p \equiv 1 \pmod{8} \end{cases}, \quad \begin{cases} p \equiv 1 \pmod{3} \\ p \equiv -1 \pmod{8} \end{cases}, \quad \begin{cases} p \equiv -1 \pmod{3} \\ p \equiv 3 \pmod{8} \end{cases}, \quad \begin{cases} p \equiv -1 \pmod{3} \\ p \equiv -3 \pmod{8} \end{cases}. \]

We solve

\[ 8b_1 \equiv 1 \pmod{3}, \quad 3b_2 \equiv 1 \pmod{8} \]

to get

\[ b_1 \equiv -1 \pmod{3}, \quad b_2 \equiv 3 \pmod{8}. \]

Now apply Chinese Remainder Theorem to get

\[ p \equiv 8 \times (-1) \times 1 + 3 \times 3 \times 1 \equiv 1 \pmod{24}, \]

\[ p \equiv 8 \times (-1) \times 1 + 3 \times 3 \times (-1) \equiv 7 \pmod{24}, \]

\[ p \equiv 8 \times (-1) \times (-1) + 3 \times 3 \times 3 \equiv 11 \pmod{24}, \]

\[ p \equiv 8 \times (-1) \times (-1) + 3 \times 3 \times (-3) \equiv 5 \pmod{24}. \]

Hence \( p \equiv 1, 5, 7, 11 \pmod{24} \).

18(a). Check that 41 is a prime. By (5.1), \( x^2 + 3x + 3 \equiv 0 \pmod{41} \) is solvable only if \( y^2 \equiv -3 \pmod{41} \) is solvable. Note that \( (-3/41) = -1 \) by 5.13(iii) since 41 \( \not\equiv 1 \pmod{6} \). So \( y^2 \equiv -3 \pmod{41} \) has no solution and thus \( x^2 + 3x + 3 \equiv 0 \pmod{41} \) has no solution.
20. Check that 61 is a prime. By (5.1), \(5x^2 - 12x + 1 \equiv 0 \pmod{61}\) is solvable only if \(y^2 \equiv 3 \pmod{61}\) is solvable. Note that by Euler’s criterion,

\[
\left( \frac{2}{61} \right) \equiv 2^{30} \equiv (2^6)^5 \equiv 3^5 \equiv -1 \pmod{61}.
\]

So \(y^2 \equiv 3 \pmod{61}\) has no solution and thus \(x^2 + 3x + 3 \equiv 0 \pmod{61}\) has no solution.

27. By (5.13)(iii), \(x^2 \equiv -3 \pmod{37}\) has a solution since \(37 \equiv 1 \pmod{6}\). Hence \(x^2 \equiv -3 \pmod{37^3}\) has exactly two solutions by (5.4).

29. Let \(a\) be a solution to \(x^{89} \equiv 3 \pmod{2200}\). Note that \(2200 = 2^3 \times 5^2 \times 11\) and \(\phi(2200) = 800\). Since

\[a^{89} \equiv 3 \pmod{2200}, \tag{4}\]

if \(d \mid a\) and \(d \mid 2200\), then \(d \mid 3\), ie. \(d = 1\) or \(3\); clearly \(d \neq 3\) since \(3 \nmid 2200\); hence \((a, 2200) = 1\). We may apply Euler’s theorem to get

\[a^{800} \equiv 1 \pmod{2200}. \tag{5}\]

Now observe that \(801 = 89 \times 9\), so multiplying (5) by \(a\) and using (4), we get

\[a \equiv a^{801} \equiv (a^{89})^9 \equiv 3^9 \equiv -117 \pmod{2200}. \tag{6}\]

For the uniqueness of solution, observe that if \(b\) is another solution, then by the same reasoning, it must also satisfy

\[b^{89} \equiv 3 \pmod{2200} \tag{6}\]

and

\[b^{800} \equiv 1 \pmod{2200}. \tag{7}\]

So \(a^{89} \equiv b^{89} \pmod{2200}\) by (4) and (6); raising this to a power of 9 and using (5) and (7) yields

\[a \equiv a^{801} = (a^{89})^9 \equiv (b^{89})^9 = b^{801} \equiv b \pmod{2200}. \]

Hence the solution is unique (modulo 2200 of course). Alternatively one may apply 3-52.