Show all of your work.

1. Find the smallest nonnegative solution for the following congruences.

\[ x \equiv 261 \mod 320 \]
\[ x \equiv 101 \mod 352 \]

**Solution:** The first line says \( x = 261 + 320k \) for some \( k \), while the second line says \( x = 101 + 352\ell \) for some \( \ell \), so we set

\[ 261 + 320k = 101 + 352\ell \]
\[ 160 = 261 - 101 = 352\ell + 320(-k). \]

This is an Exam 1 problem, and we can solve for \( \ell \) and \(-k\) provided that \((352, 320)|160\). We compute Bezout’s identity for 352 and 320:

\[ 352 = 320 + 32 \]
\[ 320 = 10 \cdot 32 + 0 \]

Thus,

\[ 160 = 5 \cdot 32 = 5 \cdot 352 + (-5) \cdot 320. \]

So we may take \( \ell = 5 \) and \(-k = -5\), or \( k = 5 \). In particular,

\[ x \equiv 101 + 5 \cdot 352 \equiv 1861 \mod [352, 320] = 352 \cdot 320 \div 32 = 3520. \]

2. What is the order of \( \overline{19} \) in \( \mathbb{Z}_n^\times \) for the following values of \( n \):

(a) \( 2^9 \).

**Solution:** \( 19 \equiv -1 \mod 4 \), and has order 2 in \( \mathbb{Z}_4^\times \), so

the order of \( \overline{19} \) in \( \mathbb{Z}_{2^9}^\times \) is \( 2|\overline{19}^2| \).

Now, \( 19^2 = 1 + 2^3 45 \), so \( \overline{19}^2 \) has order \( 2^{9-3} = 2^6 \) in \( \mathbb{Z}_{2^9}^\times \), so \( \overline{19} \) has order \( 2 \cdot 2^6 = 2^7 \).

(b) \( 5^7 \).

**Solution:** \( \overline{19} \equiv -1 \mod 5 \) so \( \overline{19} \) has order 2 in \( \mathbb{Z}_5^\times \).

So the order of \( \overline{19} \) in \( \mathbb{Z}_{5^7}^\times \) is \( 2|\overline{19}^2| \). Here, we use that \( 19^2 = 1 + 5^1 \cdot 72 \), so that \( \overline{19}^2 \) has order \( 5^{7-1} = 5^6 \) in \( \mathbb{Z}_{5^7}^\times \). So \( \overline{19} \) has order \( 2 \cdot 5^6 \) there.

(c) \( 7^{10} \).

**Solution:** \( \overline{19} \equiv 5 \mod 7 \), which has order 6 in \( \mathbb{Z}_7^\times \), so

the order of \( \overline{19} \) in \( \mathbb{Z}_{7^{10}}^\times \) is \( 6|\overline{19}^6| \).

Now, \( 19^6 = 1 + 7^3 \cdot 137160 \), and \( (7, 137160) = 1 \), so the order of \( \overline{19}^6 \) is \( 7^{10-3} = 7^7 \) in \( \mathbb{Z}_{7^{10}}^\times \). So \( \overline{19} \) has order \( 6 \cdot 7^7 \) there.
Exam 2 Solutions

(d) \(2^9 \cdot 5^7 \cdot 7^{10}\). Solution: We take the least common multiple of the answers in parts (a)–(c), so the order is

\[[2^7, 2 \cdot 5^6, 6 \cdot 7^7] = 2^7 \cdot 3 \cdot 5^6 \cdot 7^7.\]

3. Find all solutions of \(x^2 \equiv 1\) in

(a) \(\mathbb{Z}_{256}\). Solution: 256 = \(2^8\). There is a specific theorem for elements of exponent 2 in \(\mathbb{Z}_p^\times\). For \(r \geq 3\) they are 1, \(2^{r-1}-1\), \(2^{r-1}+1\) and \(-1\). In this case, that gives 1, 127, 129 and \(-1\).

(b) \(\mathbb{Z}_{275}\). Solution: 275 = \(25 \cdot 11\). Of course \(\bar{x}^2 = \bar{1}\) in \(\mathbb{Z}_{275}^\times\) if and only if \(x^2 \equiv 1\) mod 275. By the Chinese Remainder Theorem,

\[x^2 \equiv 1 \text{ mod } 275 \iff \begin{cases} x^2 \equiv 1 \text{ mod } 25 \\ x^2 \equiv 1 \text{ mod } 11 \end{cases} \iff \begin{cases} x \equiv \pm 1 \text{ mod } 25 \\ x \equiv \pm 1 \text{ mod } 11. \end{cases}\]

We can solve this explicitly using the Chinese Remainder Theorem. Here, Bezout’s identity gives

\[1 = 4 \cdot 25 + (-9) \cdot 11.\]

Case 1. \(x \equiv 1\) mod 25 and \(x \equiv 1\) mod 11. Here, \(x \equiv 1\) mod 275.

Case 2. \(x \equiv -1\) mod 25 and \(x \equiv 1\) mod 11. Here,

\[x \equiv 1 \cdot 100 + (-1) \cdot (-99) \equiv 199 \text{ mod } 275.\]

Case 3. \(x \equiv 1\) mod 25 and \(x \equiv -1\) mod 11. This is the negative of Case 2, so

\[x \equiv -199 \equiv 76 \text{ mod } 275.\]

Case 4. \(x \equiv -1\) mod 25 and \(x \equiv -1\) mod 11. Here, \(x \equiv -1\) mod 275.

4. What are the orders of the following elements of \(\mathbb{Z}_{53}^\times\)? Solution: Since 53 is prime, the orders must all divide 52, so the possible orders are 1, 2, 4, 13, 26 and 52.

(a) \(2\). Solution: \(2^2 = 4\), \(2^4 = 16\), \(2^8 = 256 = 44 = -9\), \(2^{12} = 16 \cdot -9 = -144 = 15\), \(2^{13} = 30 = -23\), \(2^{26} = 23^{2} = 529 = -1\). So 2 has order 52.

(b) \(23\). Solution: From the above calculations, we see that \(23\) has order 4.
(c) \(\mathbb{10}\). \text{Solution:} \quad 10^2 = -6, \quad 10^4 = 36 = -17, \quad 10^8 = 172 = 289 = 24, \quad 10^{12} = -17 \cdot 24 = -408 = -37 = 16, \quad 10^{13} = 160 = 1. \text{So } \mathbb{10} \text{ has order 13.}

5. Find a generator of \(\mathbb{Z}_{5310}^\times\), without explicitly calculating any numbers larger than \(2^{42}\). \text{Solution:} \quad \text{We use the results of the previous problem. Since } 23 \text{ has order 4 in } \mathbb{Z}_{53}^\times \text{ its order in } \mathbb{Z}_{5310}^\times \text{ is } 4 \cdot |23^4|, \text{ where the latter order is calculated in } \mathbb{Z}_{5310}^\times. \text{ Now } 23^4 = 1 + 53 \cdot 5280, \text{ and } (5280, 53) = 1. \text{ So the order of } 23 \text{ in } \mathbb{Z}_{5310}^\times \text{ is } 53^{10} - 1. \text{ Thus, the order of } 23 \text{ in } \mathbb{Z}_{5310}^\times \text{ is } 53^{9}. \text{ Similarly, the order of } \mathbb{10} \text{ in } \mathbb{Z}_{5310}^\times \text{ is } 13 \cdot |\mathbb{10}|^{13}. \text{ Now, } 10^{13} = 1 + 53 \cdot 188679245283, \text{ and } (53, 188679245283) = 1. \text{ So the order of } \mathbb{10} \text{ in } \mathbb{Z}_{5310}^\times \text{ is } 53^{9}. \text{ Now } \phi(53^{10}) = 52 \cdot 53^9, \text{ and that will be the order of a generator. And } 53 = 13 \cdot 4, \text{ with } (13, 4) = 1. \text{ If we find } \bar{a} \text{ and } \bar{b} \text{ with } (|\bar{a}|, |\bar{b}|) = 1, \text{ then } |\bar{a} \cdot \bar{b}| = |\bar{a}| \cdot |\bar{b}|, \text{ so if } |\bar{a}| \cdot |\bar{b}| = \phi(53^{10}), \text{ then } \bar{a} \bar{b} \text{ is the desired generator.}

In a general group } G, \text{ if an element } g \in G \text{ has order } n \text{ and if } k \text{ divides } n, \text{ then }
\begin{align*}
|g^k| &= \frac{|g|}{(|g|, k)} = \frac{n}{(n, k)} = \frac{n}{k},
\end{align*}
\text{where the last equality is because } k \text{ divides } n. \text{ In particular, both } \mathbb{10}^{53^9} \cdot 23 \text{ and } \mathbb{10} \cdot 23^{53^9} \text{ are generators for } \mathbb{Z}_{5310}^\times.

6. True or False. If false, give a counterexample. If true show why:
- For any \(\bar{a}, \bar{b} \in \mathbb{Z}_5^\times\),
  \[|\bar{a} \cdot \bar{b}| = [|\bar{a}|, |\bar{b}|],\]
i.e., the order of \(\bar{a} \cdot \bar{b}\) is equal to the least common multiple of the orders of \(\bar{a}\) and \(\bar{b}\).
\text{Solution:} \quad \text{False. Take } \bar{a} = 2 \text{ and } \bar{b} = 3. \text{ We have } 2 \cdot 3 = 1, \text{ which has order 1. But } 2 \text{ and } 3 \text{ each have order 4, so the lcm of their orders is 4.}