PROBLEM SET 6: MODULAR ARITHMETIC
(DUE NOVEMBER 8)

HARM DERKSEN

Problem 1.
(a) Do 31.3-1 in the book.
(b) Do 31.3-3 in the book.

solution
(a) The tables for addition in $\mathbb{Z}_4$ and multiplication in $\mathbb{Z}_5^*$ are

\[
\begin{array}{c|ccc}
+ & 0 & 1 & 2 \\
0 & 0 & 1 & 2 \\
1 & 2 & 3 & 0 \\
2 & 3 & 0 & 1 \\
3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{c|cccc}
+ & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 \\
2 & 2 & 4 & 1 & 3 \\
3 & 3 & 1 & 4 & 2 \\
4 & 4 & 3 & 2 & 1 \\
\end{array}
\]

We have $\alpha([0]_4) = \alpha([0]_4 + [0]_4) = \alpha([0]_4) \cdot \alpha([0]_4)$. The only element $a$ in $\mathbb{Z}_5^*$ with $a \cdot a = a$ is $a = [1]_5$. Therefore we must have $\alpha([0]_4) = [1]_5$. We also have $[1]_5 = \alpha([0]_4) = \alpha([2]_4 + [2]_4) = \alpha([2]_4) \cdot \alpha([2]_4)$. The only elements $a$ in $\mathbb{Z}_5^*$ with $a \cdot a = [1]_5$ are $a = [1]_5$ and $a = [4]_5$. Since we already have $\alpha([0]_4) = [1]_5$, we must have $\alpha([2]_4) = [4]_5$. For $\alpha([1]_4)$ we can only choose $[2]_5$ or $[3]_5$. Both choices give a solution. Let us define $\alpha([0]_4) = [1]_5$, $\alpha([1]_4) = [3]_5$, $\alpha([2]_4) = [4]_5$ and $\alpha([3]_4) = [2]_5$. One can check now that indeed $\alpha([i]_4 + [j]_4) = \alpha([i]_4) \cdot \alpha([j]_4)$ for all $i, j \in \{0, 1, 2, 3\}$.

(b) $\phi(p^e)$ is the number of elements in the set $S = \{1, 2, \ldots, p^e\}$ which are relatively prime to $p^e$. An integer is relatively prime to $p^e$ if and only if it is not divisible by $p$. The elements in $S$ divisible by $p$ are $\{p, 2p, \ldots, p^{e-1} \cdot p\}$. There are $p^{e-1}$ elements in $S$ which are not relatively prime to $p^e$. Therefore, there are $p^e - p^{e-1}$ elements in $S$ which are relatively prime to $p^e$. This shows that $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$.

Problem 2.
(a) Do 31.5-1 in the book.
(b) Do 31.5-2 in the book. (*Hint: You could first try to find an integer $a$ such that $a \equiv 1 \, (\text{mod} 9)$ and $a \equiv 2 \, (\text{mod} 8)$.*)

Solution:
(a) Using the Euclidean algorithm for example, one finds $1 = 11 - 2 \cdot 5$. This means that $11 \equiv 1 \, (\text{mod} 5)$ and $11 \equiv 0 \, (\text{mod} 11)$ and $-10 \equiv (0 \, \text{mod} 5)$ and
\(-10 \equiv 1 \pmod{11}\). Now take \(x = 4 \cdot 11 + 5 \cdot (-10) = 44 - 50 = -6\). Then \(x \equiv 4 \pmod{5}\) and \(x \equiv 5 \pmod{11}\). To get all solutions, we need \(x \equiv -6 \pmod{55}\), so \(x = -6 + 55k\) with \(k \in \mathbb{Z}\).

(b) Actually the numbers in the problem are chosen in such way that it is easy to see that \(x = 10\) is a solution. the the general solution is \(x = 10 + 9 \cdot 8 \cdot 7 \cdot k = 10 + 504k\). (In general one would not get away as easily. Consider the problem \(x \equiv a \pmod{9}\), \(x \equiv b \pmod{8}\), \(x \equiv c \pmod{7}\). First one could find a solution \(y\) such that \(y \equiv a \pmod{9}\) and \(y \equiv b \pmod{8}\). Then one could solve \(x \equiv y \pmod{72}\) and \(x \equiv c \pmod{7}\).)

**Problem 3.**

(a) What are the last 2 digits of \(7^{5555}\)? (In other words, what is \(7^{5555} \pmod{100}\). You can use Euler’s Theorem and/or the modular exponentiation algorithm.)

(b) Do problem 31.6-3 in the book.

**Solution:**

(a) \(\phi(100) = \phi(2^2 \cdot 5^2) = 2(2-1)5(5-1) = 40\). We compute \(5555 \pmod{40} = 35\), so \(7^{5555} \equiv 7^{35} \pmod{100}\). Use now the modular exponentiation algorithm. 35

\[
\begin{array}{ccccccc}
1 & 0 & 0 & 0 & 1 & 1 & \\
7 & 49 & 1 & 1 & 7 & 43 & \\
\end{array}
\]

So \(7^{5555} \equiv 7^{35} \equiv 43 \pmod{100}\).

(b) By Euler’s Theorem we have \(a^{\phi(n)} \equiv 1 \pmod{n}\). This means that \(a^{\phi(n)-1} \cdot a \equiv 1 \pmod{n}\) so \(a^{-1} \equiv a^{\phi(n)-1} \pmod{n}\). We can compute \(a^{-1}\) by computing \(a^{\phi(n)-1}\) using the modular exponentiation algorithm.

**Problem 4. *(Halloween bonus problem)* Compute \(5^{5666} \pmod{666}\). (Note that \(666 = 2 \cdot 3^2 \cdot 37\)).**

**Solution:** Note that \(5^{5666} \equiv 5^a \pmod{666}\) where \(a = 5^{666} \pmod{\phi(666)}\). \(\phi(666) = (2-1)3(3-1)(37-1) = 2 \cdot 3 \cdot 36 = 2^3 \cdot 3^2 = 216\). We need to find \(5^{666} \pmod{216}\). We again use Euler’s Theorem. \(\phi(216) = \phi(2^3 \cdot 3^3) = 2^2(2-1)3^2(3-1) = 2^3 \cdot 3^2 = 72\). 

\(666 \pmod{72} = 18\) so \(5^{666} \equiv 5^{18} \pmod{216}\). We have to compute \(5^{18} \pmod{216}\) by the modular exponentiation algorithm:

\[
\begin{array}{ccccccc}
1 & 0 & 0 & 1 & 0 & \\
5 & 25 & 193 & 53 & 1 & \\
\end{array}
\]

So \(5^{18} \equiv 1 \pmod{216}\) and

\(5^{5666} \equiv 5^{5^{18}} \equiv 5^1 \pmod{666}\)

and

\[5^{5666} \pmod{666} = 5.\]