Solutions to Assignment 3

Barr 2.1, p.66, #3 a, c, f

3. In each of the following, find q and r such that b = qm + r, according to the division principle.

(a) b = 127, m = 7

$127 = (18)7 + 1,$

(c) b = 1024, m = 16.

$1024 = (64)16 + 0,$

(f) b = -123, m = 124

$-123 = (-1)124 + 1.$

Barr 2.2, p.81, #4.

4. Solve the following pairs of congruences for a and b.

(a) $4a + b \equiv 11 \pmod{26}$

$a + b \equiv 6 \pmod{26}$

It is easy to see a = 19, b = 13.

(b) $22a + b \equiv 1 \pmod{26}$

$13a + b \equiv 5 \pmod{26}$

It is easy to see a = 14, b = 5.

C1.

(a) Compute 5^{-1} (mod 23)

Recall that the multiplicative inverse of an integer a modulo m is an integer b such that $ab \equiv 1 \pmod{m}$. We define a^{-1} by $a^{-1} = b$ MOD m.

By Trial and Error we quickly see that $(5)(14) = 70 = 3 \times 23 + 1 \equiv 1 \pmod{23}$.

So, $5^{-1} \pmod{23} = 14$.

(b) Compute 5^{-1} (mod 27)

$(5)(11) = 55 = 2 \times 27 + 1 \equiv 1 \pmod{27}$

So, $5^{-1} \pmod{27} = 11$.

C2.

(a) Find the two solutions X between 0 and 7 to $X^2 \equiv 2 \pmod{7}$.

By Trial and Error we quickly see $3^2 = 9 \equiv 2 \pmod{7}$, and $4^2 = 16 \equiv 2 \pmod{7}$.

Thus the two solutions are X = 3 and X = 4.

(b) Find the four solutions Y between 0 and 15 to $Y^2 \equiv 4 \pmod{15}$.

The four solutions are Y = 2, 7, 8 or 13.

(c) Find all solutions Z between 0 and 27 to $Z^2 \equiv 4 \pmod{27}$.

Testing all values from 0 to 27 we see that the only solutions to $Z^2 \equiv 4 \pmod{27}$ are 2 and 25.

C3.*

(a) Find a positive integer A which solves all three of:

$A \equiv 1 \pmod 3$, $A \equiv 3 \pmod 5$, and $A \equiv 5 \pmod 7$.

Brute Force Method:

$A \equiv 1 \pmod 3 \Rightarrow A = 3x + 1$ for some integer x. So, the possible values of A are 1, 4, 7, 10, 13…

$A \equiv 3 \pmod 5 \Rightarrow A = 5y + 3$ for some integer y. So, the possible values of A are 3, 8, 13, 18,…

$A \equiv 5 \pmod 7 \Rightarrow A = 7z + 5$ for some integer z. So, the possible values of A are 5, 12, 19, 26,…

Keep writing out terms until you see a term that satisfies all 3 equations.

Following this procedure eventually yields A = 103 as a solution.

Alternative Method:

First, solve $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$ using the brute force method but write up terms only upto the lowest common multiple (l.c.m) of 3 and 5 = 15

So $A \equiv 1 \pmod 3$ yields A = 1,4, 7, 10, 13, and
$A \equiv 3 \pmod 5$ yields A = 3, 8 ,13.

We see A = 13 solves both $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$.
Next, writing more terms we see the next A that solves both $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$ is $A = 28 = 15(1) + 13$. Continuing, we see $A = 43 = 15(2) + 13$ is the next solution. Thus, we see $A \equiv 13 \pmod{15}$ solves both $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$.

In general, the following is always true:

if $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$, and if x = b is a solution for both $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$, then the general solution to $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ is $x \equiv b \pmod{[m_1, m_2]}$ where $[m_1,m_2]$ denotes the lowest common multiple of m_1 and m_2.

So, since A = 13 is a solution for both $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$, the general solution to $A \equiv 1 \pmod 3$ and $A \equiv 3 \pmod 5$ is $A = 13 \pmod{15}$, since the lowest common multiple of 3 and 5 is 15.

Now, we solve $A \equiv 13 \pmod{15}$ and $A \equiv 5 \pmod 7$. Again writing out terms upto the lowest common multiple of 7 and 15 = 105, we see 103 is a solution. Thus, the general solution to $A \equiv 1 \pmod 3$, $A \equiv 3 \pmod 5$, and $A \equiv 5 \pmod 7$ is
$A \equiv 103 \pmod{105}$.

(b) Find a positive integer B which solves all of
$B \equiv 5 \pmod 6$, $B \equiv 7 \pmod{10}$, $B \equiv 2 \pmod{15}$.

$B \equiv 5 \pmod 6 \Rightarrow B = 6x + 5$ for some integer x. So, the possible values of B are 5, 11, 17,…
$B \equiv 7 \pmod{10} \Rightarrow B = 10y + 7$ for some integer y. So, the possible values of B are 7 , 17, 27,…
$B \equiv 2 \pmod{15} \Rightarrow B = 15z + 2$ for some integer z. So, the possible values of B are 2, 17, 32,…

We see that B = 17 satisfies all 3 equations so we're done.

(c) Why are there no integers C which solve both
$C \equiv 7 \pmod{10}$ and $C \equiv 8 \pmod{16}$?

$C \equiv 7 \pmod{10} \Rightarrow C = 7 + 10x$ for some integer x.
$C \equiv 8 \pmod{16} \Rightarrow C = 8 + 16y$ for some integer y.

Note that $C = 7 + 10x$ only yields odd values for C, and
$C = 8 + 16y$ only yields even values for C.

Since C cannot be both odd and even, we conclude there is no integer C which solves both $C \equiv 7 \pmod{10}$ and $C \equiv 8 \pmod{16}$.

C4.*

(a) Use Euclid's Algorithm to determine the G.C.D. (greatest common divisor) of 98944 and 184747.

```
184747 = 94944(1) + 85803
98944  = 85803(1) + 13141
85803  = 13141(6) + 6957
13141  = 6957(1)  + 6184
6957   = 6184(1)  + 773
6184   = 773(8)   + 0
```

Since 773 is the last non-zero remainder, we conclude that the G.C.D of 98944 and 184747 is 773.

(b) Compute $98945^2 \pmod{184747}$

Recall that asking to compute $98945^2 \pmod{184747}$ is equivalent to calculating the remainder when 98945^2 is divided by 184747.

Using a calculator, we see $98945^2 / 184747 \approx 52992.00001$

Thus, the Remainder = $98945^2 - (184747)(52992) = 1$

Thus, $98945^2 \pmod{184747} = 1$.