MTH 505: Number Theory — Spring 2020
Homework 3 — Drew Armstrong

Problem 1. Chinese Remainder Theorem. Find all integers $c \in \mathbb{Z}$ satisfying the following system of simultaneous congruences:

$$\begin{cases} c & \equiv 3 \bmod 5, \\ c & \equiv 6 \bmod 9, \\ c & \equiv 8 \bmod 11. \end{cases}$$

There are two ways to do this.

Two at a time. Recall that the general solution to $c \equiv a \bmod m$ and $c \equiv b \bmod n$ with $\gcd(m,n) = 1$ is $c \equiv any + bmx \bmod mn$, where $x, y \in \mathbb{Z}$ are any integers satisfying $mx + ny = 1$. First we consider $c \equiv 5 \bmod 5$ and $c \equiv 6 \bmod 9$. In this case we have $(a,b) = (3,6)$ and $(m,n) = (5,9)$. We observe that the integers $(x,y) = (2,-1)$ satisfy $mx + ny = 1$. Therefore the general solution is

$$c \equiv any + bmx = 3 \cdot 9 \cdot (-1) + 6 \cdot 5 \cdot 2 \equiv 33 \bmod 45.$$

Next we consider the two congruences $c \equiv 8 \bmod 11$ and $c \equiv 33 \bmod 45$. This time we have $(a,b) = (8,33)$ and $(m,n) = (11,45)$, and we observe that the integers $(x,y) = (-4,1)$ satisfy $mx + ny = 1$. Therefore the general solution is

$$c \equiv any + bmx = 8 \cdot 45 \cdot 1 + 33 \cdot 11 \cdot (-4) \equiv -1092 \equiv 393 \bmod 495.$$

All at once. Alternatively, recall that for any integers satisfying $\gcd(m_1, m_2, m_3) = 1$, there exist some integers $x_1, x_2, x_3 \in \mathbb{Z}$ satisfying $x_1 m_2 m_3 + m_1 x_2 m_3 + m_1 m_2 x_3 = 1$. Then for any integers $a_1, a_2, a_3 \in \mathbb{Z}$, the general solution to the congruences $c \equiv a_i \bmod m_i$ is given by

$$c \equiv a_1 x_1 m_2 m_3 + a_2 m_1 x_2 m_3 + a_3 m_1 m_2 x_3 \mod m_1 m_2 m_3.$$

In our case we have $(a_1, a_2, a_3) = (3,6,8)$ and $(m_1, m_2, m_3) = (5,9,11)$. Then by inspection[1] we observe that the integers $(x_1, x_2, x_3) = (-1,1,1)$ satisfy the desired property:

$$x_1 m_2 m_3 + m_1 x_2 m_3 + m_1 m_2 x_3 = 99 x_1 + 55 x_2 + 45 x_3 = 1.$$

Therefore the general solution is

$$\begin{aligned} c &\equiv a_1 x_1 m_2 m_3 + a_2 m_1 x_2 m_3 + a_3 m_1 m_2 x_3 \bmod m_1 m_2 m_3 \\ &\equiv 3 \cdot 99 \cdot (-1) + 6 \cdot 55 \cdot 1 + 8 \cdot 45 \cdot 1 \bmod 405 \\ &\equiv 393 \bmod 405. \end{aligned}$$

Problem 2. Application of Bézout's Lemma. For any $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$, Bézout's Lemma tells us that $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

(a) Prove the converse. That is, if $ax + by = 1$ for some $x, y \in \mathbb{Z}$, prove that $\gcd(a,b) = 1$.
(b) Apply Bézout and part (a) to prove that

$$\gcd(ab, c) = 1 \quad \Longleftrightarrow \quad \gcd(a,c) = 1 \quad \text{and} \quad \gcd(b,c) = 1.$$

[1] It inspection didn't work we would use the matrix Euclidean algorithm.

(a): Let $ax + by = 1$ and $\gcd(a, b) = d \geqslant 1$. Since $d|a$ and $d|b$ we have $a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$. But then we also have

$$1 = ax + by = da'x + db'y = d(a'x + b'y),$$

which since $d \geqslant 1$ implies that $d = 1$.

(b): Suppose that $\gcd(ab, c) = 1$, so Bézout's identity implies that $abx + cy = 1$ for some integers $x, y \in \mathbb{Z}$. But then part (a) implies $\gcd(a, c) = 1$ because $a(bx) + c(y) = 1$ and $\gcd(b, c) = 1$ because $b(ax) + c(y) = 1$. Conversely, suppose that $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, so Bézout's identity implies that $ax+cy = 1$ and $bx'+cy' = 1$ for some integers $x, y, x', y' \in \mathbb{Z}$. But then we have

$$\begin{aligned}(ax + cy)(bx' + cy') &= 1\\ abxx' + axcy' + cybx' + cycy' &= 1\\ ab(xx') + c(axy' + ybx' + ycy') &= 1,\end{aligned}$$

hence from part (a) we conclude that $\gcd(ab, c) = 1$.

Problem 3. GCD and LCM. Let $2 = p_1 < p_2 < p_3 < \cdots$ be the sequence of all primes. Then every positive integer $a \geqslant 2$ can be expressed in the form

$$a = p_1^{a_i} p_2^{a_2} p_3^{a_3} \cdots ,$$

and is uniquely determined by the sequence of exponents $a_1, a_2, a_3, \ldots$.

(a) Prove that $a|b$ if and only if $a_i \leqslant b_i$ for all i.
(b) Prove that $\gcd(a, b)_i = \min(a_i, b_i)$ for all i.
(c) Prove that $\operatorname{lcm}(a, b)_i = \max(a_i, b_i)$ for all i.
(d) Combine (b) and (c) to prove that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. [Hint: $(ab)_i = a_i + b_i$.]

(a): Suppose that $a_i \leqslant b_i$ for all i, which means that $b_i = a_i + k_i$ for some non-negative integers $k_i \geqslant 0$. It follows that

$$b = p_1^{a_1+k_1} p^{a_2+k_2} p_3^{a_3+k_3} \cdots = (p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots)(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots) = a(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots),$$

and hence $a|b$. Conversely, suppose that $a|b$ and consider the prime p_i. Then since $p_i^{a_i}$ divides a, it also divides b. But we know that $b = p_i^{b_i} m$ for some m satisfying $\gcd(m, p_i) = 1$ and hence $\gcd(m, p_i^{a_i}) = 1$. Thus we conclude from Euclid's Lemma that $p_i^{a_i} | p_i^{b_i}$, and hence $a_i \leqslant b_i$.

(b) and (c): For all integers $d \geqslant 1$ and for all primes p_i we have

$$\begin{aligned} d_i \leqslant \gcd(a, b)_i &\Leftrightarrow d| \gcd(a, b) && \text{part (a)}\\ &\Leftrightarrow d|a \text{ and } d|b\\ &\Leftrightarrow d_i \leqslant a_i \text{ and } d_i \leqslant b_i && \text{part (a)}\\ &\Leftrightarrow d_i \leqslant \min(a_i, b_i),\end{aligned}$$

which implies that $\gcd(a, b)_i = \min(a_i, b_i)$. Similarly, for all integers m we have

$$\begin{aligned} \operatorname{lcm}(a, b)_i \leqslant m_i &\Leftrightarrow \operatorname{lcm}(a, b)|m && \text{part (a)}\\ &\Leftrightarrow a|m \text{ and } b|m\\ &\Leftrightarrow a_i \leqslant m_i \text{ and } b_i \leqslant m_i && \text{part (a)}\\ &\Leftrightarrow \max(a_i, b_i) \leqslant m_i,\end{aligned}$$

which implies that $\operatorname{lcm}(a, b)_i = \max(a_i, b_i)$.

(d): For all integers $m, n \in \mathbb{Z}$ and for all primes p_i we note that $(mn)_i = m_i + n_i$. Furthermore, if $m_i = n_i$ for all primes p_i then we note that $m = n$. Thus we conclude from (b) and (c) that

$$\begin{aligned} [\gcd(a,b) \cdot \mathrm{lcm}(a,b)]_i &= \gcd(a,b)_i + \mathrm{lcm}(a,b)_i \\ &= \min(a_i, b_i) + \max(a_i, b_i) \\ &= a_i + b_i && \text{think about it} \\ &= (ab)_i, \end{aligned}$$

and hence $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = ab$.

Problem 4. RSA Cryptosystem. The following message has been encrypted using the RSA cryptosystem with public key $(n, e) = (55, 23)$:

$$[17, 1, 33, 15, 1, 13, 20, 20, 9, 39, 26, 2, 14, 49, 13, 8, 2, 15, 1, 11]$$

Decrypt the message. [Hint $A = 1$, $B = 2$, $C = 3$, etc.]

Each message is represented by a number $0 \leqslant m < 55$. (In this case, I only used numbers 1 through 26, corresponding to letters of the alphabet.) To encrypt the message I computed $c \equiv m^e \bmod n$. To decrypt the message you should compute $m \equiv c^d \bmod n$, where d is the decryption exponent.

Recall that the decryption exponent is defined by $d \equiv e^{-1} \bmod (p-1)(q-1)$, where $n = pq$. To find d, we first factor $n = 55$ to obtain the primes $p = 5$ and $q = 11$. Now we need to find $d \equiv 23^{-1} \bmod 40$, and we do this using the Euclidean algorithm. Each row corresponds to a true equation $23x + 40y = z$:

x	y	z
0	1	40
1	0	23
−1	1	17
2	−1	6
−5	3	5
7	−4	1

We conclude that $23 \cdot 7 \equiv 40 \cdot 4 + 1 \equiv 1 \bmod 40$, and hence $d = 7$. Finally, we raise each encrypted message c to the power of 7 mod 40. The resulting numbers are

$$[8, 1, 22, 5, 1, 7, 15, 15, 4, 19, 16, 18, 9, 14, 7, 2, 18, 5, 1, 11],$$

which translate to the following letters:

$$[h, a, v, e, a, g, o, o, d, s, p, r, i, n, g, b, r, e, a, k].$$