Fall 2021 – Math 328K – 55385

# Homework 7 Solutions

**Problem 1.** Use the Chinese Remainder Theorem and Hensel's Lemma to find all solutions of the following polynomial equations.

a) $x^2 + x + 34 = 0$ in $\mathbb{Z}/81\mathbb{Z}$

b) $x^2 + x + 47 = 0$ in $\mathbb{Z}/2401\mathbb{Z}$

c) $x^6 - 2x^5 - 35 = 0$ in $\mathbb{Z}/6125\mathbb{Z}$

**Solution 1.**

a) Let $f(x) = x^2 + x + 34$, with derivative $f'(x) = 2x + 1$. We compute the solutions of $f(x) = 0$ modulo 3, 9, 27, and 81.

Modulo 3, we have $f(x) \bmod 3 = x^2 + x + 1 \bmod 3$, so $f([0]_3) = [1]_3$, $f([1]) = [0]_3$ and $f([2]) = [1]_3$. This means $[1]_3$ is the only solution in $\mathbb{Z}/3\mathbb{Z}$.

To find which lifts of $[1]_3$ to $\mathbb{Z}/9\mathbb{Z}$ are solutions, we use Hensel's Lemma. Since $[f'(1)]_3 = [0]_3$ we are in the first case of Hensel's Lemma, i.e. every lift is a solution, or none of them. The lifts are $[1]_9$, $[4]_9$ and $[7]_9$. Since $f([1]_9) = [1 + 1 + 34]_9 = [0]_9$, $[1]_9$ is a solution, and therefore $[4]_9$ and $[7]_9$ are also solutions. These are all solutions modulo 9.

The lifts of $[1]_9$ to $\mathbb{Z}/27\mathbb{Z}$ are $[1]_{27}, [10]_{27}, [19]_{27}$. Since $f([1]_{27}) = [1+1+34]_{27} = [9]_{27}$, none of these are solutions. The lifts of $[4]_9$ are $[4]_{27}, [13]_{27}, [22]_{27}$. Since $f([4]_{27}) = [16+4+34]_{27} = [0]_{27}$, all of these are solutions. The lifts of $[7]_9$ are $[7]_{27}, [16]_{27}, [25]_{27}$. Since $f([7]_{27}) = [49 + 7 + 34]_{27} = [9]_{27}$, so none of these are solutions. Therefore, the solutions modulo 27 are $[4]_{27}, [13]_{27}, [22]_{27}$.

The lifts of $[4]_{27}$ to $\mathbb{Z}/81\mathbb{Z}$ are $[4]_{81}, [31]_{81}, [58]_{81}$. Since $f([4]_{81}) = [16 + 4 + 34]_{81} = [54]_{81}$, none of these are solutions. The lifts of $[13]_{27}$ are $[13]_{81}, [40]_{81}, [67]_{81}$. Since $f([13]_{81}) = [169 + 13 + 34]_{81} = [54]_{81}$, none of these are solutions. The lifts of $[22]_{27}$ are $[22]_{81}, [49]_{81}, [76]_{81}$. Since $f([22]_{81}) = [484 + 22 + 34]_{81} = [54]_{81}$, none of these are solutions. So there are no solutions in $\mathbb{Z}/81\mathbb{Z}$.

b) Let $g(x) = x^2 + x + 47$, then $g'(x) = 2x + 1$. Since $2401 = 7^4$, we again find solutions of $g(x) = 0$ modulo 7, $7^2 = 49$, $7^3 = 343$, and finally $7^4$.

To find solutions in $\mathbb{Z}/7\mathbb{Z}$, we can just try out all possibilities, or use that

$$[g(a)]_7 = [a^2 + a - 2]_7 = [(a-1)(a+2)]_7.$$

So if $[a]_7$ is a solution, then $7 \mid (a-1)(a+2)$, so either $7 \mid a-1$ or $7 \mid a+2$. So the two solutions in $\mathbb{Z}/7\mathbb{Z}$ are $[1]_7$ and $[-2]_7 = [5]_7$.

Now $[g'(1)]_7 = [3]_7$ and $[g'(5)]_7 = [0]_7$, so $[3]_7$ has a unique lift to $\mathbb{Z}/7^k\mathbb{Z}$ which is a solution, for all $k$, while we have to use the first case of Hensel's Lemma for $[5]_7$.

To find the lifts of $[1]_7$ which is are solutions, we compute $-[g'(1)]_7^{-1}[\frac{g(1)}{7}]_7 = -[3]_7^{-1}[7]_7 = [0]_7$, so $[1 + 0 \cdot 7]_{49} = [1]_{49}$ is the solution in $\mathbb{Z}/49\mathbb{Z}$. Next, $-[g'(1)]_7^{-1}[\frac{g(1)}{49}]_7 = -[3]_7^{-1}[1]_7 = [2]_7$, so $[1 + 2 \cdot 49]_{343} = [99]_{343}$ is the solution in $\mathbb{Z}/343\mathbb{Z}$. Finally, $-[g'(1)]_y^{-1}[\frac{g(99)}{343}]_7 = [2]_7$, so $[99 + 2 \cdot 343]_{2401} = [785]_{2401}$ is the solution in $\mathbb{Z}/2401\mathbb{Z}$. Indeed, a quick check with a calculator confirms that $[g(785)]_{2401} = [617057]_{2401} = [0]_{2401}$.

To find the lifts of $[5]_7$ which are solutions, we use the same strategy as in a). The lifts of $[5]_7$ in $\mathbb{Z}/49\mathbb{Z}$ are

$$[5]_{49}, [12]_{49}, [19]_{49}, [26]_{49}, [33]_{49}, [40]_{49}, [47]_{49}.$$

Since $[g(5)]_{49} = [41]_{49}$, none of these are solutions. So the only solution to $g(x) = 0$ in $\mathbb{Z}/2401\mathbb{Z}$ is $[785]_{2401}$.

c) Since $6125 = 5^3 \cdot 7^2$ we first find solutions modulo 5, $5^2$, $5^3$, 7, and $7^2$, and then use the Chinese Remainder Theorem to put them together to solutions modulo 6125.

Let $h(x) = x^6 - 2x^5 - 35$, then $h'(x) = 6x^5 - 10x^4$. Note that $[h(x)]_5 = [x^2 - 2x]_5 = [x(x-2)]$ by Fermat's little theorem, so the solutions in $\mathbb{Z}/5\mathbb{Z}$ are $[0]_5$ and $[2]_5$. We have $[h'(0)]_5 = [0]_5$ and $[h'(2)]_5 = [2]_5$.

The lifts of $[0]_5$ to $\mathbb{Z}/25\mathbb{Z}$ are $[0]_{25}, [5]_{25}, [10]_{25}, [15]_{25}, [20]_{25}$. Since $[h(0)]_{25} = [15]_{25}$, none of these are solutions modulo 25.

We have $-[h'(2)]_5^{-1} \cdot [\frac{h(2)}{5}]_5 = [2]_5 \cdot [-7]_5 = [1]_5$, so $[2 + 1 \cdot 5]_{25} = [7]_{25}$ is the solution modulo 25. Furthermore, $-[h'(2)]_5^{-1} \cdot [\frac{h(7)}{25}]_5 = [2]_5 \cdot [\frac{(7-2)\cdot 7^5 - 5 \cdot 7}{5^2}]_5 = [2]_5 \cdot [\frac{7\cdot(7^4-1)}{5}]_5 = [\frac{2\cdot 7 \cdot 2400}{5}]_5 = [0]_5$, so $[7 + 0 \cdot 25]_{125} = [7]_{125}$ is the unique solution in $\mathbb{Z}/125\mathbb{Z}$.

To find solutions modulo 7 and 49, note that $[h(x)]_7 = [x^5(x-2)]_7$, so the only solutions in $\mathbb{Z}/7\mathbb{Z}$ are $[0]_7$ and $[2]_7$. Then $[h'(0)]_7 = [0]_7$ and $[h'(2)]_7 = [32]_7 = [4]_7$.

The lifts of $[0]_7$ to $\mathbb{Z}/49\mathbb{Z}$ are $[0], [7], [14], [21], [28], [35], [42]$. Since $[h(0)]_{49} = [-35]_{49} \neq [0]_{49}$, none of them are solutions. We have $-[h'(2)]_7^{-1} \cdot [\frac{h(2)}{7}]_7 = -[4]_7^{-1} \cdot [\frac{-35}{7}]_7 = -[2]_7 \cdot [-5]_7 = [3]_7$, so the unique solution modulo 49 is $[2 + 3 \cdot 7]_{49} = [23]_{49}$.

Finally, we use the Chinese Remainder Theorem to construct the unique solution in $\mathbb{Z}/6125\mathbb{Z}$ out of the solutions $[7]_{125}$ and $[23]_{49}$. To this end, we need to find the inverses of $[125]_{49}$ and $[49]_{125}$. It is easy to guess that $[5]_{49}^{-1} = [10]_{49}$ and $[7]_{125}^{-1} = [18]_{125}$, so $[125]_{49}^{-1} = [10^3]_{49} = [20]_{49}$ and $[49]_{125}^{-1} = [18^2]_{125} = [74]_{125}$. Hence the unique solution modulo $\mathbb{Z}/6125\mathbb{Z}$ is

$$[7 \cdot 49 \cdot 74 + 23 \cdot 125 \cdot 20]_{6125} = [82882]_{6125} = [3257]_{6125}.$$

Indeed, $3257^6 - 2 \cdot 3257^5 - 35 = 1192998192645855725500$ is divisible by 6125.

**Problem 2.** Find all solutions $x \in \mathbb{Z}$ of the following systems of congruences

a)

$$\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

b)

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 5x &\equiv 2 \pmod{6} \\ 3x &\equiv 4 \pmod{7} \\ x &\equiv 5 \pmod{8} \end{aligned}$$

**Solution 2.**

a) We have $[11]_{17}^{-1} = [-3]_{17}$ and $[17]_{11}^{-1} = [2]_{11}$, so by the CRT

$$[x]_{187} = [4 \cdot 17 \cdot 2 + 3 \cdot 11 \cdot (-3)]_{187} = [37]_{187}$$

The solutions are all integers of the form $x = 37 + 187k$, for $k \in \mathbb{Z}$.

b) Assume $x$ solves the system of congruences. Since $[5]_6^{-1} = [5]_6$ the second equation is equivalent to $[x]_6 = [10]_6$. This implies $[x]_2 = [0]_2$. On the other hand, the fourth equation implies $[x]_2 = [1]_2$. This is a contradiction, so there is no solution.

**Problem 3.** Show that for any $n \in \mathbb{Z}_+$ there are $n$ consecutive integers

$$a, a+1, \ldots, a+(n-1)$$

such that each of them is divisible by a perfect square (an integer of the form $x^2$, where $x$ is an integer greater than 1).

*Hint: Find an integer $a$ such that $a+(i-1)$ is divisible by $p_i^2$ where $p_i$ is the $i$-th prime number, for all $i \in \{1, \ldots, n\}$. That is, $a$ is divisible by 4, $a+1$ is divisible by 9, $a+2$ is divisible by 25, etc.*

**Solution 3.** Let $p_i$ be the $i$–th prime number, and let $M = \prod_{i=1}^{n} p_i^2$. By the Chinese Remainder Theorem, there exists $x \in \mathbb{Z}/M\mathbb{Z}$ with

$$(x \bmod p_1^2, x \bmod p_2^2, \dots, x \bmod p_n^2) = ([0]_{p_1^2}, [-1]_{p_2^2}, \dots, [-n+1]_{p_n^2}).$$

Let $a$ be any integer with $x = [a]_M$. Then $p_1^2 \mid a$, $p_2^2 \mid a+1$, etc., up to $p_n^2 \mid a+(n-1)$.

**Problem 4.** Let $a, b \in \mathbb{Z}$ be coprime. Show that for every $c \in \mathbb{Z}$ there exists $n \in \mathbb{Z}$ such that

$$(an+b, c) = 1.$$

*Hint: use the Chinese Remainder Theorem to find $n$ such that $(an+b) \bmod p = 1 \bmod p$ for every prime factor $p$ of $c$ that does not divide $a$.*

**Solution 4.** Let $\{p_1, \dots, p_k\}$ be the set of primes which divide $c$, but not $a$, with $p_i \neq p_j$ for $i \neq j$. Let $M = p_1 \cdots p_k$. By the CRT there is $x \in \mathbb{Z}/M\mathbb{Z}$ with

$$x \bmod p_i = [a]_{p_i}^{-1}[1-b]_{p_i}$$

for all $i \in \{1, \dots, k\}$. Note that $[a]_{p_i}$ is invertible since we assumed $p_i \nmid a$. Let $n \in \mathbb{Z}$ be a representative of $x$, that is $x = [n]_M$. Then $[an+b]_{p_i} = [1]_{p_i}$ for all $i$.

Now assume that $(an+b, c) > 1$. Then there is a prime number $p$ dividing $(an+b, c)$. In particular, $p \mid c$ and $p \mid an+b$. We distinguish two cases: if $p \mid a$, then $p$ divides $b = (an+b) - an$, which is a contradiction to $a, b$ being coprime. On the other hand, if $p \nmid a$, then $p = p_i$ for some $i \in \{1, \dots, k\}$, so $[an+b]_p = [1]_p$. But we also know $[an+b]_p = [0]_p$. This is also a contradiction, so $(an+b, c) = 1$.

**Problem 5.** The goal of this problem is to prove a generalization of the Chinese Remainder Theorem for integers which are not pairwise coprime.

a) Let $m_1, m_2$ be any integers greater than 1, and set $M = \operatorname{lcm}(m_1, m_2)$ and $m = \gcd(m_1, m_2)$. Show that the map

$$\begin{aligned} f\colon \quad \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ a \bmod M &\mapsto (a \bmod m_1, a \bmod m_2) \end{aligned}$$

is well–defined and injective. Show that its image is

$$f(\mathbb{Z}/M\mathbb{Z}) = \{(x_1, x_2) \mid x_1 \bmod m = x_2 \bmod m\}.$$

b) *(optional)* Let $m_1, \dots, m_n$ be integers greater than 1 and let $M$ be the least common multiple of all of them. Show that the map

$$\begin{aligned} \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \\ a \bmod M &\mapsto (a \bmod m_1, \dots, a \bmod m_n) \end{aligned}$$

is well–defined and injective, and that its image is

$$\{(x_1, \dots, x_n) \mid x_i \bmod m_{ij} = x_j \bmod m_{ij} \text{ for all } 1 \le i, j \le n\},$$

where $m_{ij} = \gcd(m_i, m_j)$.

*Hint: use part a) and induction.*

**Solution 5.**

a) We showed in class that the maps $\mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}, a \bmod M \mapsto a \bmod m_i$ are well–defined when $m_i \mid M$. The map $f$ is just composed of these.

To show injectivity, assume that $x \in \mathbb{Z}/M\mathbb{Z}$ and $a \in \mathbb{Z}$ with $x = [a]_M$, such that $f(x) = ([0]_{m_1}, [0]_{m_2})$. This means $m_1 \mid a$ and $m_2 \mid a$. If we write

$$m_1 = p_1^{i_1} \cdots p_k^{i_k}, \qquad m_2 = p_1^{j_1} \cdots p_k^{j_k}$$

for distinct primes $p_1, \dots, p_k$ and $i_1, \dots, i_k, j_1, \dots, j_k \ge 0$. we see that $p_\ell^{i_\ell} \mid a$ and $p_\ell^{j_\ell} \mid a$ for each $\ell \in \{1, \dots, k\}$, so $p_\ell^{\max\{i_\ell, j_\ell\}} \mid a$ for each $\ell$. But this means that

$$p_1^{\max\{i_1, j_1\}} \cdots p_k^{\max\{i_k, j_k\}} \mid a$$

(using Lemma ???). So $M \mid a$, i.e. $x = [0]_M$.

Now if $x, x' \in \mathbb{Z}/M\mathbb{Z}$ with $f(x) = f(x')$, then it is easy to see that $f(x - x') = ([0]_{m_1}, [0]_{m_2})$, and so by the above $x - x' = [0]_M$, i.e. $x = x'$. So $f$ is injective.

Let

$$A = \{(x_1, x_2) \mid x_1 \bmod m = x_2 \bmod m\}.$$

It is easy to see that $f(\mathbb{Z}/M\mathbb{Z}) \subset A$: this is because

$$(a \bmod m_1) \bmod m = a \bmod m = (a \bmod m_2) \bmod m.$$

For fixed $x_1 \in \mathbb{Z}/m_1\mathbb{Z}$, the set of $x_2 \in \mathbb{Z}/m_2\mathbb{Z}$ such that $(x_1, x_2) \in A$ has exactly $m_2/m$ elements. So $|A| = m_1 m_2/m = M$ (see the question from the midterm exam). But since $f$ is injective, we also have $|f(\mathbb{Z}/M\mathbb{Z})| = M$. Therefore, $f(\mathbb{Z}/M\mathbb{Z}) = A$.