Math 328K. Fall 2025

Some solutions to Homework # 8

Prof. Hector E. Lomeli

Section 6.1. Exercise 10. Given that $11 \nmid 6$, we have $(6, 11) = 1$. Using FLT, we have that $6^{10} \equiv 1 \pmod{11}$. We also have that $2000 = 10\ell$, where $\ell = 200$. We conclude that

$$6^{2000} = \left(6^{10}\right)^{\ell} \equiv (1)^{\ell} = 1 \pmod{11}.$$

Section 6.1. Exercise 14. The last digit of the base 7 expansion of 3^{100} is the remainder 3^{100} **mod** 7. First, by FLT, we have that $3^6 \equiv 1 \pmod 7$. Also, $100\,\mathbf{mod}\,6 = 4$. In fact, we can write $100 = 6 \cdot 16 + 4$. From these considerations, we have the following computation.

$$3^{100} \equiv 3^{96}3^4 = (3^6)^{16}\, 3^4 \equiv 3^4 \pmod 7.$$

Now $3^2 \equiv 2 \pmod 7$ and hence $3^4 \equiv 4 \pmod 7$. We conclude that $3^{100}\,\mathbf{mod}\,7 = 4\,\mathbf{mod}\,7 = 4$.

Section 6.1. Exercise 18. If $3 \nmid n$ then, by FLT we have that $3^2 \equiv 1 \pmod 3$. We also know that, if n is odd, then $n^2 \equiv 1 \pmod 8$. Given that 3 and 8 are coprime, the CRT implies that $n^2 \equiv 1 \pmod{24}$.

Section 6.1. Exercise 22. First we notice that $30 = 2 \cdot 3 \cdot 5$. The numbers 2, 3, 5 are pairwise coprime. Let $n \in \mathbb{Z}$. Using FLT, we know that

$$n^2 \equiv n \pmod 2, \qquad n^3 \equiv n \pmod 3, \qquad n^5 \equiv n \pmod 5.$$

This implies that $n^3 \equiv n^2 \equiv n \pmod 2$. Using the CRT we conclude that $n^3 \equiv n \pmod 6$. We also have that

$$n^9 \equiv n^3 \equiv n \pmod 6,$$

and

$$n^9 \equiv n^5 \equiv n \pmod 5.$$

Using the CRT we conclude that $n^9 \equiv n^5 \equiv n \pmod{30}$.

Section 6.1. Exercise 28. If p, q are two different primes them $p \nmid q$ and $q \nmid p$. Let $x = p^{q-1} + q^{p-1}$. Then FLT implies that

$$x \equiv q^{p-1} \equiv 1 \pmod p, \qquad x \equiv p^{q-1} \equiv 1 \pmod q.$$

Given that $(p, q) = 1$, we conclude that $x \equiv 1 \pmod{pq}$.

Section 6.3. Exercise 8. We notice that $63 = 7 \cdot 9$. The numbers $7, 9$ are pairwise coprime. Let $a \in \mathbb{Z}$ such that $3 \nmid a$ or $9 \mid a$. Using the CRT, it is enough to show

$$a^7 \equiv a \pmod 7, \qquad a^7 \equiv a \pmod 9.$$

FLT implies that $a^7 \equiv a \pmod 7$. For the second congruence, we have to consider two cases.

- If $3 \nmid a$, then $(a, 9) = 1$ and hence $a^{\phi(9)} \equiv 1 \pmod 9$. We have that $\phi(9) = 6$, so

$$a^7 = a^6 \cdot a \equiv 1 \cdot a = a \pmod 9.$$

- If $9 \mid a$, then $a \equiv 0 \pmod 9$. This clearly implies that $a^7 \equiv a \pmod 9$.

Using the CRT we conclude that $a^7 \equiv a \pmod{63}$.

Section 6.3. Exercise 10. Let a, b be relatively prime positive integers. Let $z = a^{\phi(b)} + b^{\phi(a)}$. Then Euler's theorem implies that

$$z \equiv b^{\phi(a)} \equiv 1 \pmod a, \qquad z \equiv a^{\phi(b)} \equiv 1 \pmod b.$$

Given that $(a, b) = 1$, we conclude that $z \equiv 1 \pmod{ab}$.

Section 6.3. Exercise 12. **a)** $x \equiv 17 \pmod{20}$. **b)** $x \equiv 4 \pmod{21}$.

9. a). If p is prime, then $p \geq 2$. Using induction, we can prove that $2^{n-1} \geq n$, for all $n \in \mathbb{N}$. This implies that $p^{n-1} \geq n$.

9. b). Solution 1. If $q > 1$, then the numbers $p, p^2, \ldots, p^n$ are n positive integers that are not coprime with m and are less than m. This implies that $p, p^2, \ldots, p^n$ are not in U_m, and hence $\#(U_m) \leq m - n$. We conclude that $\phi(m) \leq m - n$. If $q = 1$, then $\phi(m) - m = \phi(p^n) - p^n = p^{n-1} \geq n$.

9. b). Solution 2. Given that $(p, q) = 1$, we have that

$$\phi(m) = \phi(p^n q) = \phi(p^n)\,\phi(q) = (p^n - p^{n-1})\phi(q).$$

This implies that

$$m - \phi(m) = p^n q - (p^n - p^{n-1})\phi(q) = p^n (q - \phi(q)) + p^{n-1}\phi(q).$$

We know that $1 \leq \phi(q) \leq q$, and $p^{n-1} \geq n$. We conclude that $m - \phi(m) \geq p^{n-1} \geq n$.

9. c). If a is an integer such that $p \mid a$, then $p^n \mid a^n$. Using the previous part of this exercise, we have that $m - \phi(m) - n \geq 0$. This implies that

$$a^{m-\phi(m)-n}$$

is an integer and

$$a^{m-\phi(m)} = a^{m-\phi(m)-n} a^n \equiv 0 \pmod{p^n}.$$

10. We will assume $m > 1$ and prove that

$$a^{m-\phi(m)}\left(a^{\phi(m)}-1\right) \equiv 0 \pmod{m}.$$

Using the FLT, we know that m can be written as

$$m = p_1^{n_1}\, p_2^{n_2}\, \cdots\, p_\ell^{n_\ell},$$

where $p_1, \ldots, p_\ell$ are distinct primes and $n_1, \ldots, n_\ell \in \mathbb{N}$.
The factors $p_1^{n_1},\ p_2^{n_2},\ \cdots,\ p_\ell^{n_\ell}$ are pairwise coprime. Using the CRT, it is enough to prove that

$$a^{m-\phi(m)}\left(a^{\phi(m)}-1\right) \equiv 0 \pmod{p_i^{n_i}},$$

for all $i = 1, \ldots, \ell$. For each i, we also define $q_i = m/p_i^{n_i}$. Clearly, $(p_i, q_i) = 1$.
Let $1 \leq i \leq \ell$ be chosen. We have two cases: $p_i \mid a$ and $p_i \nmid a$.

Case 1. If $p_i \mid a$, then we can write $m = p_i^{n_i}\, q_i$. Using the previous problem, we have that

$$a^{m-\phi(m)} \equiv 0 \pmod{p_i^{n_i}}.$$

Case 2. If $p_i \nmid a$, then $(p_i^{n_i}, a) = 1$. Using Euler's theorem,

$$a^{\phi\left(p_i^{n_i}\right)} \equiv 1 \pmod{p_i^{n_i}}.$$

However, we also have that $(p_i^{n_i}, q_i) = 1$ and therefore,

$$\phi(m) = \phi(p_i^{n_i})\phi(q_i).$$

This implies that

$$\left(a^{\phi(m)}-1\right) \equiv 0 \pmod{p_i^{n_i}}.$$

In both cases, we conclude that

$$a^{m-\phi(m)}\left(a^{\phi(m)}-1\right) \equiv 0 \pmod{p_i^{n_i}}.$$