Solutions for Unit 6

Solution for PS6-1. When $\gcd(a, m) \neq 1$, the number a has no inverse modulo m, nor can any positive power of a be congruent to 1 modulo m.

I used the 'egcd' Python function from the lecture notes to compute GCDs and, as a result, inverses when they exist. For the powers, I used some trial and error.

number	**inverse**	**power congruent to 1**
1	1	$1^1 \equiv 1$
10	$\nexists$	$\nexists$
13	7	$13^4 \equiv 1$
19	19	$19^2 \equiv 1$
27	$\nexists$	$\nexists$
29	29	$29^2 \equiv 1$

Solution for PS6-2. Let $n = q(p-1)+r$, where $q, r \in \mathbb{Z}$ and $0 \le r < p-1$. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Therefore,

$$a^n = (a^{p-1})^q \cdot a^r \equiv 1^q a^r = a^{n \bmod (p-1)} \pmod{p}.$$

Solution for PS6-3. Suppose that $a, b \in \mathbb{Z}_m^*$ and $c = ab \bmod m$. We must show that $c \in \mathbb{Z}_m^*$.
By the Inverse Existence Theorem, a^{-1} and b^{-1} exist. Therefore,

$$c \cdot (b^{-1}a^{-1}) = abb^{-1}a^{-1} \equiv 1 \pmod{m},$$

so c^{-1} exists. By the Inverse Existence Theorem, $\gcd(c, m) = 1$, so $c \in \mathbb{Z}_m^*$.

Solution for PS6-4.

a. First, check that f_a is indeed a function from $\mathbb{Z}_m^*$ to $\mathbb{Z}_m^*$. Of course, for any $m \in \mathbb{Z}_m^*$, $ax \bmod m$ is a unique defined value in $\mathbb{Z}_m$; the only question is whether it lies in $\mathbb{Z}_m^*$. By the result of ***PS6-3***, it does.
To prove that f_a is a *bijection*, we demonstrate that it has an inverse function. By the Inverse Existence Theorem, $\exists\, b \in \mathbb{Z}_m^*$ such that $ab \equiv 1 \pmod{m}$. Now, for all $x \in \mathbb{Z}_m^*$,

$$f_b(f_a(x)) = b(ax \bmod m) \bmod m = bax \bmod m = x\,,$$

so $f_b \circ f_a = \mathrm{id}$. Similarly, $f_a \circ f_b = \mathrm{id}$. This completes the proof.

b. Let $L = (b_1, b_2, \ldots, b_{\phi(m)})$ be a list of all the elements of $\mathbb{Z}_m^*$. By the previous part, the list

$$L' = (ab_1 \bmod m, ab_2 \bmod m, \ldots, ab_{\phi(m)} \bmod m)$$

consists of the same elements as L, but perhaps in a different order. Comparing the products of the elements in each list,

$$b_1 b_2 \cdots b_{\phi(m)} \equiv a^{\phi(m)} b_1 b_2 \cdots b_{\phi(m)} \pmod{m}.$$

By the Inverse Existence Theorem, each b_i has an inverse b_i^{-1}. Multiplying both sides by $b_1^{-1} b_2^{-1} \cdots b_{\phi(m)}^{-1}$ gives $1 \equiv a^{\phi(m)} \pmod{m}$.

c. When m is a prime, every nonzero number in $\mathbb{Z}_m$ is coprime to m, so $\mathbb{Z}_m^* = \{1, 2, \ldots, m-1\}$ and $\phi(m) = m-1$. The congruence now reads $a^{m-1} \equiv 1 \pmod{m}$, which is exactly Fermat's Little Theorem.

Solution for PS6-5.

a. By definition, $P_{m,a}$ is an infinite sequence, but all its elements lie in the finite set $\mathbb{Z}_m^*$. Therefore, there must be a repetition in the sequence. Let $i < j$ be two positions such that $a^i \bmod m = a^j \bmod m$. By the Inverse Existence Theorem, a has an inverse b modulo m. So,

$$a^i \equiv a^j \pmod m \implies b^i a^i \equiv b^i a^j \pmod m \implies 1 \equiv a^{j-i} \pmod m.$$

Thus, 1 reappears in the sequence at position $j - i$.

b. Let k be the smallest positive index at which 1 appears in $P_{m,a}$. Then $a^k \equiv 1 \pmod m$. For any index $\ell > k$, let $\ell = qk + r$ with $q, r \in \mathbb{N}$ and $0 \le r < k$. Then

$$a^\ell = (a^k)^q \cdot a^r \equiv 1^q a^r = a^r \pmod m.$$

Therefore, $P_{m,a}$ consists of the block $(a^0 \bmod m, \dots, a^{k-1} \bmod m)$ repeated infinitely often.

c. Let's look more closely at the argument in Part ***a.*** If we consider the first $m+1$ elements in the sequence, there must already be a repetition because the elements come from a set of size $\le m$. Therefore, we can enforce $0 \le i < j \le m$ in that argument.

Thus, 1 reappears at position $j - i \le m$. So the value of k in the previous part—which is the period—is $\le m$.

d. Look even more closely at the argument above. The elements in the sequence in fact come from the set $\mathbb{Z}_m^*$, whose cardinality is $\phi(m) \le m - 1$. Therefore, $k \le m - 1$. In particular, the period cannot be m.

Note: With a little more effort, you can in fact show that $k \mid \phi(m)$, so the period must be a divisor of $\phi(m)$.

Alternate Solution for PS6-5.

a. Since $a \in \mathbb{Z}_m^*$, by Euler's Theorem, $a^\phi(m) \equiv 1 \pmod m$. Since $\phi(m) > 0$, we see that 1 reappears in the sequence at position $\phi(m)$.

b. Same as above.

c. The period is clearly at most $\phi(m)$. Since $\mathbb{Z}_m^* \subset \mathbb{Z}_m$, it follows that $\phi(m) < m$. So the period is $\le m$.

d. Of course, we've in fact shown that the period is $< m$. In particular, it can't be m.

Solution for PS6-6. Consider an arbitrary $a \in \mathbb{Z}_{pq}$. The positive divisors of pq are $1, p, q$, and pq. So $\gcd(a, pq)$ must be one of these four numbers. Let's count how many numbers a lead to each of these GCDs.

Case 1. $\gcd(a, pq) = 1$. Then $a \in \mathbb{Z}_{pq}^*$. By definition, there are $\phi(pq)$ such numbers a.

Case 2: $\gcd(a, pq) = pq$. Since $a < pq$, this means $a = pq$, i.e., there is exactly one possibility for a.

Case 3: $\gcd(a, pq) = p$. Then $p \mid a$ and $a < pq$, so $a \in \{p, 2p, 3p, \dots, (q-1)p\}$, i.e., $q - 1$ possibilities for a.

Case 4: $\gcd(a, pq) = q$. Analogously, there are $p - 1$ possibilities for a in this case.

Since there is no overlap between the cases and there are $|\mathbb{Z}_{pq}| = pq$ total possibilities for a, we obtain

$$pq = \phi(pq) + 1 + (q-1) + (p-1).$$

Solving for $\phi(pq)$ gives $\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

Solution for PS6-7.

a. We work modulo p. Imagine drawing an arrow from each $a \in \mathbb{Z}_p^*$ to a^{-1}. Then the arrow from a^{-1} will point to $(a^{-1})^{-1} = a$. We can then pair off a and a^{-1}. If we consider any other element $b \notin \{a, a^{-1}\}$, then $\{b, b^{-1}\}$ will be another pair disjoint from $\{a, a^{-1}\}$.

There is a catch: a might equal a^{-1} sometimes! But by ***PS5-9***[HW], this only happens for $a = 1$ and $a = p - 1$. So the argument above works for all $a \in S$.

b. Consider the modulo-p product Q of all numbers in S. We can rearrange the product to place each $a \in S$ adjacent to its partner $a^{-1} \in S$. The product within each pair is 1 modulo p. Therefore, so is the overall product, i.e., $Q \equiv 1 \pmod p$. Therefore,

$$(p-1)! = 1 \times Q \times (p-1) \equiv 1 \times 1 \times (-1) \equiv -1 \pmod p.$$

c. By the definition of congruence, the last statement above can be rewritten as $p \mid (p-1)! + 1$.

Solution for PS6-8. Since m is composite, we can write $m = ab$ where $2 \le a \le m-1$ and $2 \le b \le m-1$. Consider the list of factors $L = (1, 2, \ldots, m-1)$ whose product equals $(m-1)!$. Three cases arise.

Case 1: $a \neq b$. In this case both a and b appear in L. Therefore $m = ab \mid (m-1)!$, whence $m \nmid (m-1)! + 1$.

Case 2: $a = b > 2$. In this case, $m = a^2 > 2a$, so a and $2a$ both appear in L. Thus, $m = a^2 \mid (m-1)!$, as before.

Case 3: $a = b = 2$. Then $m = 4$ and we check directly that $4 \nmid 3! + 1 = 7$.

Solution for PS6-9.

a. By the GCD Linear Combination Theorem (LCT), $\exists\, k, \ell \in \mathbb{Z}$ such that $\gcd(a,b) = ka + \ell b$. By ***PS5-6*** ^{HW},

$$\frac{n}{\operatorname{lcm}(a,b)} = \frac{n \cdot \gcd(a,b)}{ab} = \frac{n(ka + \ell b)}{ab} = \frac{kn}{b} + \frac{\ell n}{a} \in \mathbb{Z},$$

since $b \mid n$ and $a \mid n$.

b. From the given info,

- $\gcd(p_1, p_2) = 1$, so n is divisible by $\operatorname{lcm}(p_1, p_2) = p_1 p_2$;
- $\gcd(p_1 p_2, p_3) = 1$, so n is divisible by $\operatorname{lcm}(p_1 p_2, p_3) = p_1 p_2 p_3$;
- and so on.

Note: Once we study mathematical induction, we'll learn a better way to write this type of proof formally.

Solution for PS6-10. We first work out the factorization $2730 = 2 \times 3 \times 5 \times 7 \times 13$. By the previous result, it suffices to show that each of these prime factors divides $n^{13} - n$.

Consider each $p \in \{2, 3, 5, 7, 13\}$. If $p \mid n$ then $p \mid n^{13}$ as well, so $p \mid n^{13} - n$. Otherwise, if $p \nmid n$, we apply Fermat's Little Theorem:

- For $p = 2$, we have $n^{13} \equiv 1^{13} \equiv 1 \equiv n \pmod 2$.
- For $p = 3$, we have $n^{13} = (n^2)^6 \cdot n \equiv 1^6 \cdot n \equiv n \pmod 3$.
- For $p = 5$, we have $n^{13} = (n^4)^3 \cdot n \equiv 1^3 \cdot n \equiv n \pmod 5$.
- For $p = 7$, we have $n^{13} = (n^6)^2 \cdot n \equiv 1^2 \cdot n \equiv n \pmod 7$.
- For $p = 13$, we have $n^{13} \equiv n \pmod{13}$.