COMP 2711H Discrete Mathematical Tools for Computer Science
Solutions to Tutorial Problems: Number Theory and Cryptography

Q1. The digit in the unit's place of a number a is $a \bmod 10$. We work modulo 10.

(a) Since $3^2 \equiv -1$, we have that

$$3^{70} \equiv (3^2)^{35} \equiv (-1)^{35} \equiv -1 \equiv 9.$$

(b) Since $9^2 \equiv 1$, we have that

$$9^{1573} \equiv 9^{2 \cdot 786} \cdot 9 \equiv (1^{786} \cdot 9) \equiv 9.$$

Q2. (a) We run Euclidean algorithm on $(1009, 17)$. We have that

$$\begin{aligned} 1009 &= 59 * 17 + 6 \\ 17 &= 2 * 6 + 5 \\ 6 &= 1 * 5 + 1. \end{aligned}$$

Then we work backwards to find the inverse of 17 modulo 1009.

$$\begin{aligned} 1 &= 6 - 5 & &= 6 - (17 - 2 * 6) \\ &= -17 + 3 * 6 & &= -17 + 3 * (1009 - 59 * 17) \\ &= 3 * 1009 - 178 * 17 \end{aligned}$$

So, the inverse of 17 modulo 1009 is $(1009 - 178) = 831$.

(b) 111

(c) 735

Q3. For any $a \in Z_m$, we know that a has inverse modulo m if and only if a and m are co-prime. Hence, to prove that at least $\sqrt{m}$ elements of Z_m do not have multiplicative inverses, it suffices to show that at least $\sqrt{m}$ elements of Z_m are not relatively prime to m. Since m is not prime, there is some integer $a \in Z_m$ such that $a|m$ and $a > 1$. Without loss of generality, we assume $a \leq \sqrt{m}$ since otherwise we can take the number m/a. Now consider $S = \{0, a, 2a, \ldots, (\lceil\sqrt{m}\rceil - 1)a\} \subseteq Z_m$. One can easily see that all these $\lceil\sqrt{m}\rceil$ numbers in S are not relatively prime to m.

Q4. Recall that an integer a is relatively prime to n if and only if a has a inverse modulo n. To prove that n is a prime, it suffices to show that for any number $a \in \{1, \ldots, n-1\}$, a is relatively prime to n, or equivalently, a has a inverse modulo n. Note that for any $a \in \{1, \ldots, n-1\}$, a is not a multiple of n. By the hypothesis, we have that

$$a^{n-1} \equiv 1 \pmod{n}.$$

Hence, $(a^{n-2} \bmod n)$ is the inverse of a modulo n. This completes the proof.

Q5. Note that $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. We can prove that $2730|n^{13} - n$ using an argument similar to that in Q8.

Q6. For any prime $p > 5$, 10 is not a multiple of p. By Fermat's little theorem, we have that

$$10^{p-1} \equiv 1 \pmod{p}.$$

Hence, for any positive integer k, we have that

$$(10^{p-1})^k \equiv 1 \pmod{p}.$$

So, $p|(10^{k(p-1)} - 1)$ for any integer $k > 0$.

Q7. As in the tutorial, the given system of congruences is equivalent to the following system.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

(a) Use the construction in the proof of Chinese remainder theorem.

- $a_1 = 0$, $a_2 = 1$, $a_3 = 3$
- $m_1 = 2$, $m_2 = 3$, and $m_3 = 5$
- $M = m_1 m_2 m_3 = 30$
- $M_1 = M/m_1 = 15$, $M_2 = M/m_2 = 10$, $M_3 = M/m_3 = 6$
- $M_1^{-1} \equiv 1 \pmod{m_1}$, $M_2^{-1} \equiv 1 \pmod{m_2}$, $M_3^{-1} \equiv 1 \pmod{m_3}$
- solution $x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} = 28$

(b) Use back substitution. From the first congruence, we know that $x = 2u$ for some integer u. Substitute this into the second congruence, we get

$$2u \equiv 1 \pmod{3}.$$

Solving this congruence, we get $u \equiv 2 \pmod{3}$. So, $u = 3s + 2$ for some integer s, and $x = 2u = 6s + 4$. Then substituting this into the third congruence, we get

$$6s + 4 \equiv 3 \pmod{5}.$$

Solving this congruence yields $s \equiv 4 \pmod{5}$. So, $s = 5t + 4$ for some integer t, and the following is a solution to the system.

$$x = 6(5t + 4) + 4 = 30t + 28.$$

So, $x \equiv 28 \pmod{30}$ is the solution to the system of congruence.

Q8.

- If part: Since $(n-1)! \equiv -1 \pmod{n}$ and $(n-1) \equiv -1 \pmod{n}$, we have that

  $$(n-1)! \cdot (n-1) \equiv 1 \pmod{n}.$$

  Note that for any number $a \in \{1, \ldots, n-1\}$,

  $$a \cdot \frac{(n-1)!}{a} \cdot (n-1) \equiv 1 \pmod{n}.$$

  a has an inverse modulo n, so a is relatively prime to n. Therefore n is a prime.

- Only-if part: When $n = 2$, the congruence obviously holds. Without loss of generality, we assume that n is a prime greater than or equal to 3. Now consider the set $\{1, 2, \ldots, (n-1)\}$. We claim that 1 and $n-1$ are the only numbers in this set, which have their inverse to be themselves. Too see this, consider the following equation.
$$a^2 \equiv 1 \pmod{n}$$
or, equivalently,
$$(a-1)(a+1) \equiv 0 \pmod{n}.$$
The roots of the equation are $a \equiv 1$ and $a \equiv -1$.
Since, for any number $a \in \{2, 3, \ldots, (n-2)\}$, a has a unique inverse a^{-1} and $a^{-1} \neq a$, we can pair a with its inverse. We get $(n-3)/2$ such pairs. So,
$$2 \cdot 3 \cdots (n-3) \cdot (n-2) \equiv 1^{(n-3)/2} \equiv 1 \pmod{n},$$
and
$$(n-1)! \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}.$$

Q9. When $n = 1$, the equation holds. Now suppose that the equation holds for $n = k$. In the inductive step, we show that the equation also holds for $n = k + 1$.

$$\begin{aligned}
1^3 + 2^3 + \cdots + (k)^3 + (k+1)^3 &= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \qquad \text{(by inductive hypothesis)} \\
&= (k+1)^2 \left[\left(\frac{k}{2}\right)^2 + (k+1)\right] \\
&= (k+1)^2 \left[\frac{k^2+4k+4}{4}\right] \\
&= (k+1)^2 \left[\frac{(k+2)^2}{4}\right] \\
&= \left[\frac{(k+1)(k+2)}{2}\right]^2
\end{aligned}$$

This completes the proof.