CS70 HW4

February 28, 2021

Contents

1 Modular Arithmetic Solutions

(a) $2x \equiv 5 \pmod{15}$.

Here since gcd(2, 15) = 1, $2^{-1} \pmod{15}$ is unique and equal to 8.
So $x \equiv 5 * 8 \equiv 40 \equiv 10 \pmod{15}$

(b) $2x \equiv 5 \pmod{16}$

Here since gcd(2, 16) = 2, and $2x = 5 + 16 * k$, for some k $\in \mathbb{Z}$. The right side of this equation is odd number, but left side is even. Thus there is no such solution for x.

(c) $5x \equiv 10 \pmod{25}$

Here $5x = 10 + 25 * k$, for some k $\in \mathbb{Z}$. So $x = 2 + 5 * k$ and in the range of [0, 24]. For all possible k, x is in the set of {2, 7, 12, 17, 22}.

2 Euclid's Algorithm

(a) The procedure is as follow:

$$\begin{aligned} gcd(527, 323) &= gcd(323, 204) \\ &= gcd(204, 109) \\ &= gcd(109, 95) \\ &= gcd(95, 14) \\ &= gcd(14, 11) \\ &= 1 \end{aligned}$$

$$\begin{aligned} gcd(527, 323) &= gcd(323, 204) \\ &= gcd(204, 119) \\ &= gcd(119, 85) \\ &= gcd(85, 34) \\ &= gcd(34, 17) \\ &= gcd(17, 0) \\ &= 17 \end{aligned}$$

(b) The procedure is as follow:

$$\begin{aligned} gcd(27, 5) &= gcd(5, 2) && [2 = 27 + (-5) * 5] \\ &= 1 && [1 = 5 + (-2) * 2] \end{aligned}$$

Use the right side of equation, we obtain

$$\begin{aligned} 1 &= 5 + (-2) * [27 + (-5) * 5] \\ &= (-2) * 27 + 11 * 5 \end{aligned}$$

So the multiplicative inverse of 5 (mod 27) is 11.

(c) The procedure is as follow:

$$\begin{aligned} 5x + 26 &\equiv 3 \pmod{27} \\ 5x &\equiv 4 \pmod{27} \\ x &\equiv 44 \pmod{27} \\ x &\equiv 17 \pmod{27} \end{aligned}$$

(d) Disprove.

a has no multiplicative inverse mod $c \implies gcd(a, c) \neq 1$. But it may still have solution. Counter example is $5x \equiv 10 \pmod{25}$, in the section 1 part (c).

3 Modular Exponentiation

(a) $13^{2018} \equiv 1 \pmod{12}$.

Since $13 \equiv 1 \pmod{12}$ and $1^{2018} \equiv 1 \pmod{12}$ is obvious.

(b) $8^{11111} \equiv 7 \pmod{9}$.

(By Fermat's Equation,)$8^8 \equiv 1 \pmod{9}$. And $11111 \equiv 7 \pmod{8}$. And $8 * 8^7 \equiv 1 \pmod{9}$, since $\gcd(8, 9) = 1$, $8^7 \pmod{9}$ is equal to the multiplicative inverse of $8 \pmod{9}$, which is 7.

$8^{11111} \equiv 8 \pmod{9}$

Since $8^2 \equiv 1 \pmod{9}$ and $8^{11111} = 8^{5555*2+1} = 8 \pmod{9}$

(c) $7^{256} \equiv 4 \pmod{11}$.

By Fermat's Equation, $7^{10} \equiv 1 \pmod{11}$. And $256 \equiv 6 \pmod{10}$, which is to compute $7^6 \pmod{11}$. $7^6 = 49 * 49 * 49 \equiv 5 * 5 * 5 \equiv 125 \equiv 4 \pmod{11}$.

(d) $3^{160} \equiv 16 \pmod{23}$.

By Fermat's Equation, $3^{22} \equiv 1 \pmod{23}$. And $160 \equiv 6 \pmod{22}$, which is to compute $3^6 \pmod{23}$. $3^6 = 9 * 81 \equiv 9 * 12 \equiv 108 \equiv 16 \pmod{23}$.

4 Euler's Totient Function

(a) Since p is a prime number, [0, 1, 2 ... p - 1] are all relatively prime to p.
Thus $\phi(p) = p - 1$.

(b) Since p is a prime, then p^k has only factor of p $\implies$ set S $\{p, 2p, \ldots, p^k\}$ are relatively not prime to p and $|S| = p^k/p = p^{k-1}$.
Thus $\phi(p^k) = p^k - p^{k-1} = (p-1) * p^{k-1}$.

(c) From part (a), $\phi(p) = p - 1$. Thus $a^{\phi(p)} = a^{p-1}$, which according to Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

(d) To prove

$$\forall i \in \{1, 2, \ldots, k\}, \quad a^{\phi(b)} \equiv 1 \pmod{p_i}$$

The key part is to solve $\phi(b)$.
Since $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, from Euler's totient function, $\phi(b) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k}) = (p_1 - 1) * p^{\alpha_1 - 1} \cdot (p_2 - 1) * p^{\alpha_2 - 1} \ldots (p_k - 1) * p^{\alpha_k - 1} = (p_1 - 1) \cdot (p_2 - 1) \ldots (p_k - 1) * K$, for some integer K $\in \mathbb{Z}$. Now since $\phi(b)$ has factors of $(p_i - 1), \forall i \in \{1, 2, \ldots, k\}$, the proof is done.

5 FLT Converse

(a) Since $gcd(n, a) \neq 1$, there exists a common factor, namely $k \geq 2$ that $n = c_0 * k$ and $a = c_1 * k$, for some $c_0, c_1, k \in \mathbb{N}$. Assume the equation $a^{n-1} \equiv 1 \pmod{n}$ holds, meaning that $\exists c_2 \in \mathbb{N}, a^{n-1} = 1 + c_2 * n \implies (c_1 * k)^{n-1} - c_0 * c_2 * k = 1$. Since the left side has common factor of k, but the right side is 1, which implies $k = 1$, that $gcd(n, a) = 1$, contradiction.

Thus for every a and n such that $\texttt{gcd}(n, a) \neq 1$, we have $a^{n-1} \not\equiv 1 \pmod{n}$.

(b) From $S(n) = \{i : 1 \leq i \leq n, \texttt{gcd}(n, i) = 1\}$, we can define two set:
$Q(n) = \{q : q \in S(n), q^{n-1} \equiv 1 \pmod{n}\}$;
$P(n) = \{p : p \in S(n), p^{n-1} \not\equiv 1 \pmod{n}\}$;
$\mid S \mid = \mid Q \mid + \mid P \mid$; If we can find $q \in P(n)$, then we can define a map T from Q(n) to P(n), T = p * q_i, for $q_i \in Q(n)$.
Now we wanna prove it's one-to-one.

Proof. Proof by contradiction.

Say $q_1 \neq q_2$, but $p * q_1 \equiv p * q_2 \pmod{n}$. Then we have $p * q_1 = p * q_2 + c_0 * n$, which is same as $p * q_1 - p * q_2 = p(q_1 - q_2) = c_0 * n$. But the since gcd(p, n) = 1, $q_1 - q_2$ must be multiple of n, which is impossible. □

Now since it's one-to-one, we obtain $\mid Q \mid$ is at least as large $\mid P \mid$. Thus $\mid Q \mid \geq \mid S \mid /2$.

(c) $a \equiv b \mod m_1 \implies a - b = c_0 * m_1$, for some $c_0 \in \mathbb{Z}$;
$a \equiv b \mod m_2 \implies a - b = c_1 * m_2$, for some $c_1 \in \mathbb{Z}$;
Since $\gcd(m_1, m_2) = 1$, a - b is multiple of m_1 and m_2, it must also be the multiple of $m_1 m_2$. Thus $a - b = c_2 * m_1 m_2$, for some $c_2 \in \mathbb{Z}$.
So $a \equiv b \pmod{m_1 m_2}$.

(d) Since $a \in S(n)$ and $n = p_1 p_2 \cdots p_k$, we have the fact that a is prime to $p_1, p_2, \cdots, p_k$. Then $a^{n-1} = a^{p_1 p_2 \cdots p_k - 1}$.
$\forall i \in \{1, 2, \ldots, k\}$, since $p_i - 1 \mid n - 1$ and also a is prime to p_i, $a^{n-1} = a^{(p_i - 1) * K} \equiv 1 \pmod{p_i}$. And since p_i are distinct primes, $gcd(p_i, p_j) = 1$ for $i \neq j$.

So $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$.

(e) From part (b), number 561 has following properties:

(1) 561 = 3 * 11 * 17 where 3, 11 and 17 are distinct primes.

(2) 560 = 2 * 280; 560 = 10 * 56; 560 = 16 * 35 $\implies (3 - 1) \mid 560, (11 - 1) \mid 560, (17 - 1) \mid 560$.

So for all a coprime with 561, $a^{560} \equiv 1 \pmod{561}$.