

CS 111 Practice Quiz 2

Solution 1:

(a) We have: $8^9 \equiv 3^9 \equiv 3 \cdot (3^2)^4 \equiv 3 \cdot (4^2)^2 \equiv 3 \cdot 1^2 \equiv 3 \pmod{5}$

(b) $\gcd(6, 13) = 1$, $6^{-1} \pmod{13}$ exists.

Find integers a, b such that: $6a = 13b + 1$

Multiples of 6: 6 12 \dots 66

Multiples of 13: 13 26 \dots 65

Thus $a = 11, b = -5 \Rightarrow 6^{-1} \equiv 11 \pmod{13}$

(c) By FLT: $5^{10} \equiv 1 \pmod{11}$. Multiply both sides by 5^{-1} gives:

$$5^{-1} \equiv 5^9 \equiv \dots \equiv 9 \pmod{11}$$

(d) Multiply both sides by 5^{-1} gives:

$$5^{-1} \cdot 5x \equiv 7 \cdot 5^{-1} \pmod{11} \Rightarrow x \equiv 7 \cdot 5^{-1} \equiv 7 \cdot 9 \equiv 8 \pmod{11}$$

Solution 2:

(a)

- Not correct, because $\phi(n) = 12 \cdot 4 = 48$ which is not coprime with $e = 3$
- Not correct, because $p = q = 11$
- Not correct, because $\phi(n) = 2 \cdot 30$ which is not coprime with $e = 5$

(b)

(i) $n = p \cdot q = 5 \cdot 11 = 55$ and $\phi(n) = (p-1)(q-1) = 4 \cdot 10 = 40$.

(ii) According to the algorithm, $d \equiv 7^{-1} \pmod{40}$.

We now compute $7^{-1} \pmod{40}$. Using the method of linear combinations, we need to find a, b such that $7a = 40b + 1$.

Multiples of 7: 7 14 \dots 161

Multiples of 40: 40 80 \dots 160

Thus $a = 23, b = -4$. This gives us $d \equiv 7^{-1} \equiv 23 \pmod{40}$.

(iii) $E(2) = 2^7 \text{ rem } 55 = 128 \text{ rem } 55 = 18$.

Solution 3:

- (a) True because $n^2 + 5n + 6 = (n + 2)(n + 3)$ which is product of two consecutive integers.
(b) True because $n^2 + 5n + 6 > 2$ for $n > 0$ and $n^2 + 5n + 6$ is even (follows from a)
-