Math 312 Section 951 Test #4 Solutions

August 4, 2023

1a ISBN-10 code is valid iff $\sum_{i=1}^{10} id_i \equiv 0 \mod 11$. To find ?, we solve

$$0 \times 1 + 1 \times 1 + \cdots + ? \times 5 + \cdots \equiv 0 \mod 11$$

$$? = 5$$

1b Similar to 1a, we have $? = 3$.

2a Notice that $\phi(n) = \phi\left(\prod_{i=1}^{k} p_i^{m_i}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$ where $\prod_{i=1}^{k} p_i^{m_i}$ is the prime factorization of n. Therefore

$$\phi(891) = \phi(3^4 \times 11) = 891 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{11}\right) = 540$$

$$\phi(4125) = \phi(5^3 \times 3 \times 11) = 4125 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{11}\right) = 2000$$

2b Note $\phi(n) = \phi\left(\prod_{i=1}^{k} p_i^{m_i}\right) = \prod_{i=1}^{k} p_i^{m_i - 1}(p_i - 1)$ and consider the possible factors of 6, we reach

$$\phi(7) = 7 - 1 = 6$$

$$\phi(14) = (2 - 1) \times (7 - 1) = 6$$

$$\phi(9) = 3 \times (3 - 1) = 6$$

$$\phi(18) = (2 - 1) \times 3 \times (3 - 1) = 6$$

3 Recall that for a given odd integer $n > 2$, let's write $n - 1$ as $2^s t$ where s is a nonnegative integer and t is an odd positive integer. Let's consider an integer b, called a base. Then, we say n passes *Miller's test* for the base b if one of following congruence relations holds:

$$b^t \equiv 1 \mod n$$

$$b^{2^r t} \equiv -1 \mod n \text{ for some } 0 \le r < s$$

In our case $25 - 1 = 2^3 \times 3$, the base is 7. Check that

$$7^{24} \equiv 1 \mod 25$$

$$7^{12} \equiv 1 \mod 25$$

$$7^{6} \equiv -1 \mod 25$$

Therefore, 25 passes *Miller's test* for the base 7. However we know that 25 is a composite. 25 must be a strong pseudoprime to the base 7.

4 By Fermat's little theorem

$$p^{q-1} \equiv 1 \mod q$$

and it is obvious that

$$q^{p-1} \equiv 0 \mod q$$

we conclude that

$$p^{q-1} + q^{p-1} \equiv 1 \mod q$$

Similarly,

$$p^{q-1} + q^{p-1} \equiv 1 \mod p$$

These two congruence relations imply that $p^{q-1} + q^{p-1} - 1$ is a multiple of both p and q. Therefore, $\mathrm{lcm}(p, q) | \left(p^{q-1} + q^{p-1} - 1\right)$, which is equivalent to

$$p^{q-1} + q^{p-1} \equiv 1 \mod pq$$

5a By Fermat's little theorem, we have

$$3^6 \equiv 1 \mod 7$$

Hence,

$$3^{6\times 16+4} \equiv 3^4 \equiv 4 \mod 7$$

5b Recall Wilson's theorem states that a natural number $n > 1$ is prime if and only if $(n-1)! \equiv -1 \mod n$. In our case, $1763 = 41 \times 43$. By Wilson's theorem we have $40! \equiv -1 \mod 41$ and $42! \equiv -1 \mod 43$. Suppose $40! \equiv a \mod 1763$, then

$$a \equiv -1 \mod 41$$

$$41 \times 42a \equiv -1 \mod 43$$

The second equation can be simplifed to

$$a \equiv 21 \mod 43$$

Use Chinese remainder theorem to solve the above system of two linear congruences, we have

$$a \equiv -1 \times 43 \times 21 + 21 \times 41 \times 21 \equiv 1311 \mod 1763$$